Bericht

des Berliner Datenschutzbeauftragten

zum 31. Dezember 1998

Der Berliner Datenschutzbeauftragte hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§ 29 Berliner Datenschutzgesetz – BlnDSG –). Der vorliegende Bericht schließt an den am 23. März 1998 vorgelegten Jahresbericht 1997 an und deckt den Zeitraum zwischen 1. Januar und 31. Dezember 1998 ab.

Erstmals werden die über Berlin hinaus bedeutsamen Dokumente in einem gesonderten Anlagenband („Dokumente zum Datenschutz 1998“) veröffentlicht, der gemeinsam mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg herausgegeben wird.

Dieser Jahresbericht ist über das Internet ***(http://www.datenschutz-berlin.de)*** *abrufbar; wir bemühen uns, dort alle im Bericht zitierten Fundstellen zugänglich zu machen.*

Impressum

Herausgeber: Berliner Datenschutzbeauftragter
Pallasstraße 25/26
10781 Berlin

Telefon: (0 30) + 78 76 88 44
Telefax: (0 30) 2 16 99 27
e-mail: mailbox@datenschutz-berlin.de
http://www.datenschutz-berlin.de

Redaktion: Volker Brozio, Laima Nicolaus

Druck: Verwaltungsdruckerei Berlin

Die Broschüre wurde auf Umwelt-Recycling-Papier gedruckt!

Inhaltsverzeichnis

Anlagen zum Jahresbericht 1998

The Governments of OECD Member Countries . . . declare that they will reaffirm their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder data flows of personal data.

Aus: Ministerial declaration on the Protection of Privacy on Global Networks, 7./9. Oktober 1998, Ottawa

Il problema non è garantire la privacy è educare chi non la vuole ad apprezzarla

Überschrift eines Artikels von Umberto Eco im L'Espresso vom 28. Mai 1998

Einleitung

Nichts verdeutlicht besser den Spannungsbogen, der von der weltweiten Wahrnehmung des Datenschutzes als Voraussetzung der Weiterentwicklung globaler Netzwerke für den elektronischen Handel *(„e-commerce")* bis zum individuellen Umgang mit den eigenen personenbezogenen Daten reicht, als diese beiden Zitate aus dem vergangenen Jahr: Hier die Erklärung der mächtigsten Industrienationen der Welt, den Datenschutz zum Gegenstand weltweiter Wirtschaftspolitik machen zu wollen – wenn auch in einer Weise, die den Handel nicht unnötig behindert –, dort die Feststellung eines der bekanntesten Schriftsteller der Gegenwart, dass nicht der Schutz der Privatsphäre, sondern die Aufgabe, die Betroffenen zur Wertschätzung ihrer eigenen Privatsphäre zu erziehen, das Problem der Gegenwart ist. Gehen die Regierungen in den Erwägungsgründen ihrer Deklaration davon aus, dass Nutzer und Konsumenten die Sicherstellung der fairen Sammlung und Verarbeitung ihrer Daten als Voraussetzung ihres Vertrauens in die Netzwerke verlangen, stellt Eco fest, dass der „gewöhnliche Mensch keine Gelegenheit verpasst, seine Daten den Hunden und Schweinen zum Fraß vorzuwerfen"[1].

Tatsächlich ist die Einstellung der Menschen zur Notwendigkeit des Schutzes ihrer Daten offensichtlich widersprüchlich. In einer *Repräsentativumfrage* von 3 000 Personen ab 14 Jahren in Deutschland, die im Frühjahr des vergangenen Jahres mit Unterstützung der Datenschutzbeauftragten von dem bekannten BAT-Freizeit-Forschungsinstitut in Hamburg unter Leitung von Prof. Horst Opaschowski durchgeführt wurde[2], wünschten sich zwar 55 % aller Befragten, dass dem Daten-

[1] Umberto Eco: L'Espresso v. 28. Mai 1998

[2] Der gläserne Konsument, Multimedia und Datenschutz. Hg. vom Freizeit-Forschungsinstitut der British-American Tobacco (Germany). Hamburg 1998

schutz künftig mehr Bedeutung zukommt (in Ostdeutschland übrigens 66 % gegenüber 52 % im Westen); 51 % fühlten sich gar hilflos gegenüber Verstößen gegen den Datenschutz. 36 % der Befragten nahmen an, dass ihre Daten schon einmal missbraucht worden waren, 24 % sogar mehrmals. Allerdings gaben 42 % der Befragten an, die Hauptursache für Verstöße gegen den Datenschutz liege im eigenen sorglosen Umgang mit den Daten. Nur (oder immerhin?) 15 % Befragte haben schon einmal Antworten auf Fragebögen unter Hinweis auf den Datenschutz verweigert. 83 % hatten nichts gegen Überwachungskameras in öffentlichen Schalterräumen einzuwenden.

Besonders die neuen Informationstechniken erwecken Argwohn: 30 % aller Computernutzer waren der Auffassung, dass sensible Daten im Computer nicht gegen einen Zugriff durch Unbefugte, z. B. über das Netz, geschützt sind. Bei einer ähnlichen Untersuchung in den *USA* einige Monate zuvor zeigte sich, dass dort die Befürchtungen noch größer sind: Deutlich über 50 % „Netzbürger“ fürchten den Missbrauch ihrer Angaben im Netz oder beim Versand von e-mails[3].

Weltweit dominierte im vergangenen Jahr in der Datenschutzdiskussion die Frage, auf welche Weise auf diese Situation zu reagieren sei: Durch mehr staatliche Regulierung oder durch Stärkung der Rechte, aber auch der Sensibilität der Betroffenen. Der deutschen – und der europäischen – Rechtstradition entspricht eher der Weg verstärkter Regulierung. Die Europäische Datenschutzrichtlinie weist in diese Richtung; über die Verpflichtung der Mitgliedsstaaten zur Umsetzung (der die Bundesrepublik im vergangenen Jahr nicht nachgekommen ist) hinaus übt sie durch ihre strengen Vorschriften zum Datenexport auch erheblichen Druck auf Drittstaaten aus, ebenfalls durch gesetzliche Regelungen für ein „angemessenes Datenschutzniveau“ zu sorgen.

Insbesondere in den USA ist der Widerstand groß: Obwohl die Datenschutzdiskussion Anfang der sechziger Jahre dort ihren Ausgangspunkt nahm, gibt es nur für die Bundesregierung[4], nicht aber für die Privatwirtschaft ein umfassendes Datenschutzrecht. Vielmehr wird dort, nachdem in den vergangenen Jahren vor dem Hintergrund der Neuen Medien die Bedeutung des Schutzes der Privatsphäre wieder erkannt worden ist, in der *Selbstregulierung* die Lösung gesehen, und zwar sowohl in Selbstverpflichtung und vertraglicher Bindung der Datenverarbeiter als auch in einer viel stärkeren Einbeziehung der Betroffenen selbst. „Notice and Choice“, Information des Betroffenen und Gelegenheit zur eigenen Entscheidung über die Verarbeitung der Daten, ist ein Schlagwort, das diese Einstellung kennzeichnet. So fremd

[3] Privacy and American Business: Commerce, Communication and Privacy Online, Hackensack, NJ 1997; vgl. auch Westin: Privacy on the Internet: Everyone a Data Protection Officer? In: Berliner Datenschutzbeauftragter (Hg.): Das Internet – Ende des Datenschutzes? Materialien zum Datenschutz. Band 26. Berlin 1998

[4] Privacy Act of 1974, Public Law 93–579, 93rd Congress, Title 54. S.C. Sec. 552 a

ist dies für unsere Rechtslage nicht: Das deutsche Grundrecht der informationellen Selbstbestimmung zielt ja gerade darauf ab, dem Betroffenen die Entscheidung über die Verarbeitung seiner Daten zu überlassen.

Dies setzt allerdings Rahmenbedingungen voraus, die sich nicht von alleine einstellen. Die Zusammenhänge moderner Informationsverarbeitung sind für die Bürger oft undurchschaubar, Verantwortungsstrukturen werden zunehmend undeutlich. Ohne ein Mindestmaß an erzwungener Transparenz, an unüberschreitbaren Grundprinzipien, an einklagbaren Rechten der Betroffenen und letztlich auch Aufsichts- und Kontrollfunktionen werden Selbstregulierungsmechanismen keinen Bestand haben. Hierzu gehört auch die Sensibilisierung der Betroffenen über die Risiken, denen sie durch die globale Informationsstruktur ausgesetzt sind. Der Widerspruch zwischen OECD-Politik und Ecos Befund wird sich auflösen, wenn beide Entwicklungslinien zueinander finden.

1. Rechtliche Rahmenbedingungen

1.1 Europa und Deutschland

Europarecht wirkt unmittelbar

Mit Bedacht haben wir die Überschrift über dieses Kapitel gegenüber den Vorjahren geändert: Europa steht nunmehr beim Überblick über die Rechtsentwicklung an erster Stelle. Mit dem 24. Oktober 1998 ist die Frist abgelaufen, innerhalb derer die Bundesrepublik verpflichtet gewesen wäre, die Europäische *Datenschutzrichtlinie* (EU-Richtlinie)[5] in innerdeutsches Recht umzusetzen. Dies ist nicht gelungen, vielmehr wurde in der vergangenen Legislaturperiode nur ein Referentenentwurf für eine *Neufassung des Bundesdatenschutzgesetzes (BDSG)* vorgelegt, der über die Beratung mit den Wirtschaftsverbänden nicht hinausgekommen ist. Die Folge ist, dass nunmehr entsprechend der Rechtsprechung des Europäischen Gerichtshofes und auch der deutschen Gerichte die Richtlinie in einem bestimmten Umfang unmittelbare Wirkung entfaltet.

Insbesondere sind alle staatlichen Stellen verpflichtet, auf die Durchsetzung der einzelnen Bestimmungen der Richtlinie hinzuwirken, soweit diese unmittelbar anwendbar sind („self executive“) und soweit das bestehende Recht eine entsprechende Anwendung zulässt *(„vertikale Wirkung“)*. Dies betrifft vor allem die Auslegung von Generalklauseln, die ja das ganze Datenschutzrecht durchziehen. So wird bei der Beurteilung der schutzwürdigen Interessen der Betroffenen (z. B. § 28 Abs. 1, S. 1 Ziff. 2 BDSG) die Richtlinie zu beachten sein. Dies betrifft vor allem die Verarbeitung der „sensiblen Daten“, also der Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit und Sexualleben (Art. 8 Abs. 1 EU-Richtlinie).

Darüber hinaus kommen den Betroffenen in der Übergangszeit erweiterte Rechte auf Widerspruch gegen die rechtmäßige Verarbeitung von Daten (Art. 14 Abs. 1 a EU-Richtlinie) und auf erweiterte Informationen von den verantwortlichen Stellen (Art. 10 c, 11 Abs. 1 c EU-Richtlinie) zu. Zu beachten ist auch, dass die Begriffsbestimmungen der Richtlinie teilweise stark von denjenigen des Bundesdatenschutzgesetzes abweichen.

Klärungsbedürftig ist, in welchem Umfang die unmittelbare Wirkung Verwaltungen betrifft, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen. Die EU-Richtlinie nennt hier ausdrücklich Titel V und VI des Vertrags über die Europäische Union, insbesondere

[5] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABlEG Nr. L 281, 31 v. 24. 11. 1995

„betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (merkwürdigerweise „einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt“) und die Tätigkeiten des Staates im strafrechtlichen Bereich“ (Art. 3 Abs. 2 EU-Richtlinie). Die Beispiele ziehen einen engen Rahmen, so dass für das deutsche Recht davon auszugehen ist, dass außer dem Verteidungsressort nur Polizei und Strafverfolgungsbehörden ausgenommen sind. Zu berücksichtigen ist, dass mit der Ratifizierung und dem In-Kraft-Treten des Amsterdamer Vertrages[6] weitere Bereiche in die „erste Säule“, in der das Gemeinschaftsrecht in vollem Umfang gilt, hinüberwandern werden.

Anders zu beurteilen ist die Frage, inwieweit aus der Datenschutzrichtlinie Konsequenzen für Privatunternehmen zu ziehen sind *(„horizontale Wirkung“)*. Der Europäische Gerichtshof hat hier im Gegensatz zur vertikalen Wirkung bisher Zurückhaltung geübt, wenn auch bislang keine Entscheidung bekannt ist, die mit hinreichender Klarheit sagt, dass im Verhältnis der Bürger untereinander bei nicht rechtzeitiger Umsetzung einer Richtlinie überhaupt keine Auswirkungen bestehen[7]. Jedenfalls sind die Aufsichtsbehörden als öffentliche Stellen wegen der sie betreffenden vertikalen Wirkung verpflichtet, auch gegenüber nichtöffentlichen Stellen darauf hinzuwirken, dass die Grundsätze der Richtlinie Beachtung finden. Für den besonders prekären Bereich des Datenexports in Drittländer haben die Aufsichtsbehörden in einer vom Berliner Datenschutzbeauftragten geleiteten Arbeitsgruppe hierfür eine Vorgehensweise abgesprochen[8].

Die allgemeine Datenschutzrichtlinie wird zunehmend ergänzt durch speziellere Richtlinien, die zumindest teilweise weitere datenschutzrechtliche Vorgaben für den deutschen Gesetzgeber enthalten: Gleichzeitig mit der EU-Datenschutzrichtlinie hätte die *Telekommunikationsrichtlinie*[9] umgesetzt werden sollen, dies ist ebenfalls nicht geschehen, sondern erst im Rahmen der Neufassung der Telekommunikations-Datenschutzverordnung geplant[10]. Ebenfalls in Kraft ist die *Fernabsatzrichtlinie*[11] mit datenschuztrechtlich relevanten Vorschriften über die Information des Kunden, den Abschluss des Vertrags im Netz oder die Zahlung mit einer Kreditkarte; eine besondere Richtlinie für den *Fernabsatz bei Finanzdienstleistungen* ist in Vorbereitung. Die Abwicklung des Geschäftsverkehrs im Internet *(„e-commerce“)* und die hierfür

[6] ABlEG 1997 Nr. C 340 S. 1
[7] z. B. EUGH Urteil v. 19. 11. 91 – Rs C-6/90 u. 9/90 („Francovich“) in: NJW 1992, 165 ff.
[8] vgl. 4.7
[9] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. 12. 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation vom 30. 1. 1998, ABlEG L 24/1
[10] vgl. 5.1
[11] Richtlinie 97/7/EG des Europäischen Parlamentes und des Rates vom 20. 5. 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz, ABlEG Nr. L 144 v. 4. 6. 1997, S. 19

unentbehrliche digitale Signatur, die im deutschen Recht bereits eine Regelung erfahren hat[12], sind weitere Gegenstände künftiger europäischer Gesetzgebung.

Rechtsentwicklung in Deutschland

Die Weiterentwicklung des deutschen Datenschutzrechtes stand naturgemäß im Vordergrund der rechtspolitischen Diskussionen des vergangenen Jahres. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte mehrfach in Beschlüssen Forderungen für die Anpassung an die EU-Richtlinie erhoben[13]. Sie beinhalten nicht nur das Anliegen, den von der Richtlinie vorgegebenen Rahmen für die Ausweitung des informationellen Selbstbestimmungsrechts so weit wie möglich zugunsten des Bürgers zu nutzen, sondern auch, die Gesetzgebung zum Anlass zu nehmen, angemessenere Regelungen für den Umgang mit der Informationstechnik zu finden. Der von der vorherigen Bundesregierung vorgelegte Entwurf entsprach dem nur sehr unvollkommen.

Die zögerliche Behandlung der Umsetzung hat verschiedenen Institutionen Gelegenheit gegeben, die Ausgestaltung des künftigen Datenschutzrechtes grundsätzlicher zu betrachten.

Der 62. Deutsche Juristentag, der vom 22. bis zum 25. September in Bremen stattfand, befasste sich in seiner Abteilung Öffentliches Recht mit der Fragestellung: „Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen?“. Prof. Michael Kloepfer, Ordinarius für Staats- und Verwaltungsrecht an der Humboldt-Unversität zu Berlin, hatte das Gutachten erstattet, das er in 46 Thesen mit weit reichenden Vorschlägen zur Fortentwicklung des Datenschutzrechtes zusammenfasste[14]. Im Mittelpunkt steht die These, bei einer grundsätzlichen Neuorientierung müsse „der Datenschutz als konstitutiver Teil einer umfassenden Informationsordnung begriffen werden, für das das – auf den Gedanken der Informationsgerechtigkeit ausgerichtete – Informationsrecht den rechtlichen Rahmen bietet“[15]. Hieraus leitete Kloepfer den Vorschlag ab, ein Informationsgesetzbuch zu entwickeln, das „als übergreifende, rechtsbereinigende und -harmonisierende Kodifikation des Informationsrechts des Bundes zu konzipieren wäre“ und in dem ein „Bundesdatengesetz“ eine Teilkodifikation

12 Gesetz zur digitalen Signatur v. 22. 7. 97, BGBl. I, 1872
13 Entschließung der 51. Konferenz v. 14./15. 3. 1996, JB 1996, Anlage 2.2; Entschließung der 54. Konferenz 23./24. 10. 1997, JB 1997, Anlage 2.3.1; Entschließung der 56. Konferenz v. 5./6. 10. 1998, JB 1998, Anlagenband „Dokumente zum Datenschutz 1998“, Teil B II
14 Michael Kloepfer: Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? Gutachten D zum 62. Deutschen Juristentag. München 1998
15 These 23, a.a.O. S. D 145

darstellen würde[16]. Er griff damit eine Idee auf, die erstmals im Jahresbericht 1990 des Berliner Datenschutzbeauftragten entwickelt worden war[17]. Nach längeren Diskussionen fasste die Abteilung Öffentliches Recht eine Reihe von Beschlüssen, die dem Votum Kloepfers folgten[18]. Die Idee eines Informationsgesetzbuchs wurde aufgegriffen, bei den Schutzstandards eine Differenzierung nach Grundrechtspositionen (z. B. Medienfreiheit, Wissenschaftsfreiheit, Glaubensfreiheit) bzw. nach spezifischen Sachstrukturen (z. B. Gesundheits- und Sozialrecht, Strafprozessrecht) gefordert, technischer Selbstschutz und Selbstregulierung (z. B. Datenschutz-Audit, Codes of conduct) wurden als Eckpfeiler der Neuregelung betrachtet. Über Kloepfer hinausgehend wurde empfohlen, „ein grundsätzlich einheitliches materielles Datenschutzrecht für den öffentlichen und den privaten Bereich zu schaffen, dessen innere Differenzierungen sich nach den Unterschieden in der Schutzbedürftigkeit unter Beachtung der Selbstbestimmung (Freiwilligkeit) und des Gefahrenpotentials zu richten haben“ – Kloepfer hatte zwar gefordert, den Schutz vor privater Datenmacht erheblich zu verbessern, aber die Auffassung vertreten, dieser dürfe dem Schutz der Datenmacht öffentlicher Stellen nicht gleichartig, vielmehr nur gleichwertig sein[19]. Eine klare Absage erteilte der Juristentag dem Versuch, den Gebrauch von Verschlüsselungstechniken durch entsprechende rechtliche Regelungen zu beschränken.

In ähnlich grundsätzlicher Weise äußerten sich im November fünf Landesdatenschutzbeauftragte, unter ihnen der Berliner Datenschutzbeauftragte, und formulierten in einem Appell an die neue Bundesregierung 10 Punkte für einen Politikwechsel zum wirksamen Schutz der Privatsphäre[20]. Neben der Forderung, in das Grundgesetz ein Grundrecht auf Datenschutz aufzunehmen, wird die umfassende Modernisierung und Effektivierung der Datenschutzgesetze verlangt, in der bereichsspezifischen Datenschutzgesetzgebung müssten statt der bisher üblichen Aufblähung von Fachgesetzen, die zugleich die datenschutzrechtliche Substanz aushöhlen, Rechtsgarantien gewährleistet werden, der Datenschutz im privaten Bereich müsse rechtlich und organisatorisch ausgebaut werden.

In der SPD-Fraktion des Bundestages wurde ein Eckwertepapier entwickelt, das zur öffentlichen Diskussion gestellt wurde[21] und das bei den bevorstehenden neuerlichen Novellierungsbemühungen in die Erörterungen einfließen wird. Dies wird sicher auch für den Entwurf eines

16 These 24, ebd.
17 JB 1990, 1.2
18 [www.datenschutz-berlin.de/doc/sonst/jurtag98.htm]
19 These 27, a.a.O. S. D 146
20 Anlagenband „Dokumente zum Datenschutz 1998“, Teil A
21 Unter Nutzung des Internet hat der Bundestagsabgeordnete Jörg Tauss hierfür ein Forum eröffnet (www.transs.de/bn.html)

Bundesdatenschutzgesetzes der Fraktion Bündnis 90/Die Grünen aus dem letzten Bundestag[22] zutreffen, der dort nicht mehr beraten wurde, dessen viele weiterführende Gedanken aber Beachtung finden sollten.

Die letzten realisierten datenschutzrechtlich relevanten Gesetzgebungsvorhaben der vergangenen Legislaturperiode waren nicht von der Zielsetzung der Fortentwicklung des Datenschutzrechtes, sondern von dem Bemühen geprägt, im Interesse der öffentlichen Sicherheit die informationelle Selbstbestimmung einzuschränken. In mehreren Änderungen der Strafprozessordnung (StPO) wurde nach vielen Jahren der Diskussion der Große Lauschangriff eingeführt, wobei auch das Grundrecht auf Unverletzlichkeit der Wohnung beschränkt wurde[23]; die Nutzung von Daten über die Gene von Straftätern (DNA-Analyse) wurde auch über laufende Ermittlungsverfahren hinaus erlaubt und beim BKA eine zentrale Gendatei eingeführt[24]. Zuvor war bereits das Begleitgesetz zum Telekommunikationsgesetz[25] in Kraft getreten, das die Möglichkeiten der Telefonüberwachung weit über den Bereich der Anbieter öffentlicher Telekommunikationsnetze ausdehnte – ohne allerdings den archaischen § 12 Fernmeldeanlagengesetz zu ändern, der die Weitergabe von Daten über die „Umstände der Telekommunikation“ (also z. B. wer mit wem wann und wo telefoniert hat) ohne inhaltliche Voraussetzungen gestattet[26]. Die seit Jahren in den Schubläden, zuletzt des Bundestages, liegende Novelle der StPO, die dort erstmals datenschutzrechtliche Vorschriften schaffen soll, ist hingegen wieder nicht vorangekommen.

Den Sicherheitsinteressen dienten auch Änderungen außerhalb der StPO: So wurde dem *Bundesgrenzschutz* die Befugnis eingeräumt, verdachtsunabhängige Kontrollen auf Verkehrswegen durchzuführen[27], die Sozialbehörden wurden ermächtigt, Angaben über den derzeitigen und künftigen Aufenthaltsort von Sozialleistungsempfängern an die Sicherheitsbehörden zu übermitteln[28].

Zwei andere große Bereiche der Justiz, bei denen seit vielen Jahren datenschutzrechtliche Defizite bestanden, verfügen seit dem vergangenen Jahr über spezialrechtliche Regelungen: Am 1. Juni ist endgültig das *Justizmitteilungsgesetz* in Kraft getreten[29], am 1. Dezember 1998 das Vierte Gesetz zur Änderung des *Strafvollzugsgesetzes,* das die Datenverarbeitung im Strafvollzug nunmehr auf eine bereichsspezifische Grundlage stellt[30].

22 Entwurf eines BDSG, BT-Drs. 13/9082
23 Gesetz zur Änderung des Grundgesetzes (Art. 13 GG) v. 26. 3. 1998, BGBl. I S. 610; Art. 2 des Gesetzes zur Verbesserung der Bekämpfung der organisierten Kriminalität v. 4. 5. 1998, BGBl. I, 845
24 Gesetz zur Änderung der Strafprozessordnung (DNA-Identitätsfeststellungsgesetz) v. 7. 9. 1998, BGBl. I, 2646, vgl. 4.3.1
25 Telekommunikationsbegleitgesetz v. 17. 12. 97, BGBl. 1997, 3108, vgl. 5.2
26 vgl. 5.2
27 Erstes Gesetz zur Änderung des Bundesgrenzschutzgesetzes v. 24. 6. 1998, BGBl. I, 2486
28 Erstes Gesetz zur Änderung des Medizinproduktgesetzes v. 6. 8. 1998, BGBl. I, 2005
29 Justizmitteilungsgesetz v. 18. 6. 1997, BGBl. I, 1430
30 BGBl. I S. 2461, vgl. 4.3.1

Erneut keinen Fortschritt gab es bei der datenschutzgerechten Gestaltung der *Abgabenordnung,* der Verfahrensvorschrift der Steuerverwaltung, für die damit weiterhin der Datenschutz unbekanntes Terrain bleibt. Das Steuergeheimnis alleine reicht nicht aus: Es schützt zwar vor der unbefugten Offenbarung von Daten, räumt den Betroffenen aber keinerlei Rechte gegenüber der Steuerverwaltung ein. Dieser Zustand ist angesichts der tiefen Eingriffe, die die Steuerverwaltung in die informationelle Selbstbestimmung vornimmt, nach wie vor nicht akzeptabel.

In der Rechtsprechung ist wiederum eine Vielzahl von Entscheidungen zu Einzelfragen mit datenschutzrechtlichem Inhalt gefällt worden. Einen gewissen Schwerpunkt bildete die Frage, in welchem Umfang *pauschale Einwilligungserklärungen* abverlangt werden dürfen und wie diese im Verhältnis zum Recht der Allgemeinen Geschäftsbedingungen stehen[31].

Das Bundesverfassungsgericht hat die mit Spannung seit Jahren ausstehende Entscheidung zu der Frage noch nicht getroffen, ob die Befugnis des *Bundesnachrichtendienstes,* auch zu Zwecken der Strafverfolgungsbehörden Fernmeldeverbindungen abzuhören und diesen die Ergebnisse mitzuteilen, verfassungsrechtlichen Bestand hat. Allerdings fand im Dezember eine mündliche Verhandlung statt, bei der auch die Datenschutzbeauftragten gehört wurden. Von der im nächsten Jahr erwarteten Entscheidung werden wichtige Erkenntnisse zur Bedeutung des Fernmeldegeheimnisses ausgehen. Weitere Entscheidungen des Gerichts zur Telefonüberwachung und zum Recht auf Auskunft über Daten der Polizei und des Verfassungsschutzes stehen ebenfalls noch aus.

Erbe der DDR

International und national wird mit großer Aufmerksamkeit verfolgt, wie im deutschen Recht mit der erschreckenden Aktenhinterlassenschaft des *Staatssicherheitsdienstes der ehemaligen DDR* umgegangen wird. Mit dem Stasi-Unterlagen-Gesetz vom 20. Dezember 1991 wurde ein bislang gut funktionierender Ausgleich zwischen den Interessen der Allgemeinheit an der Aufarbeitung der Stasi-Hinterlassenschaft und den Rechten Betroffener und Dritter gefunden. Zunächst stand im Mittelpunkt der öffentlichen Aufmerksamkeit die nunmehr erstmalig gegebene Möglichkeit, für die Betroffenen, d. h. die von der Staatssicherheit Ausgeforschten, die von einem jenseits jeglicher rechtsstaatlicher Normen agierenden Geheimdienst gesammelten Informationen einsehen zu können. Die Betroffenen konnten feststellen, wer, was, wann und bei welcher Gelegenheit an Informationen über sie zusammentrug und der DDR-Staatssicherheit zutrug.

31 z. B. OLG Frankfurt, Urteil v. 26. 2. 1998 1 U 171/96, In: RDV 98, S. 175

Der Gesetzgeber hatte aber auch erkannt, dass eine faktisch unbegrenzte Aufbewahrung dieser „Schnüffeldaten“ über Millionen von Bürgern eine nicht unerhebliche Gefährdung des Persönlichkeitsrechts der Betroffenen darstellt. Verfassungsrechtlich dürfte daher kaum zu begründen sein, dass ein herausragendes Allgemeininteresse daran besteht, alle gesammelten Daten ohne Unterschied und unbefristet in personenbezogener Form vorzuhalten. Um diesen Grundrechtseingriff abzumildern, enthielt § 14 Stasi-Unterlagen-Gesetz von 1991 eine Regelung zur *Anonymisierung* und Löschung personenbezogener Informationen über Betroffene und Dritte. Diese Vorschrift gab diesen Personen, also nicht den „Tätern“, ab 1. Januar 1997 einen *Anspruch auf Anonymisierung* (Schwärzung) oder Vernichtung ihrer personenbezogenen Unterlagen, wenn eine Schwärzung sich technisch als nicht durchführbar erweisen sollte. Da bekanntlich fast alle personenbezogenen Stasi-Akten auch Informationen über Dritte (beispielsweise Familienangehörige, Freunde oder Kollegen) enthalten, wurden weitere Einschränkungen des Rechts auf Anonymisierung eingefügt.

Im Dezember 1996 schob der Bundesgesetzgeber diese Frist um zwei weitere Jahre hinaus, da ein Beginn der Anonymisierung aufgrund der noch nicht vollständigen Erschließung der Aktenbestände praktisch nicht möglich war. Ende des Jahres 1998 wurde erneut von verschiedenen Seiten vorgetragen, dass eine Anonymisierung ab dem 1. Januar 1999 noch nicht möglich sei, da die Behörde des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes mit der Bearbeitung einer größeren Anzahl von Anonymisierungsanträgen extrem überlastet wäre. Dem trug der Bundesgesetzgeber Rechnung und verlängerte die Frist – letztmalig, wie es in der Begründung hieß – bis zum Jahr 2003[32].

Aus datenschutzrechtlicher Sicht wird die weitere Verschiebung der Anonymisierungsregelung des Stasi-Unterlagen-Gesetzes immer problematischer. Auch nach Ablauf einer erneuten Fristverlängerung im Jahre 2003 dürfte die gegenwärtige Anonymisierungsregelung wegen des Informationsumfanges und der Informationsverknüpfungen unter gleichbleibender Berücksichtigung möglicher Interessen aller in den Akten verzeichneten betroffenen Opfer und Dritten regelmäßig nicht durchführbar sein. Der Bundesgesetzgeber ist also gefordert, andere Lösungen zu suchen.

1.2 Datenschutz in Berlin

Im Gegensatz zu anderen Bundesländern, die im vergangenen Jahr bereits die EU-Richtlinie umgesetzt[33] oder diese zumindest in Angriff genommen haben, rieten wir in Berlin zur Zurückhaltung. Zum einen zeigen Erfahrung mit dem derzeitigen *Berliner Datenschutzgesetz,* das ebenfalls vor dem Bundesdatenschutzgesetz novelliert wurde, dass bei dieser Reihenfolge Abweichungen vom später geschaffenen Bundesrecht in Kauf genommen werden müssen, die häufig zu Anwendungsschwierigkeiten führen. Dies betrifft weniger materielle Abweichungen, mit denen ein Land eine gegenüber dem Bund datenschutzfreundlichere Einstellung zum Ausdruck bringt. Es betrifft vielmehr vor allem strukturelle und terminologische Fragen, die wenig substanziellen Gehalt haben, aber die Rechtsanwendung erheblich erschweren. Zum anderen würde eine sehr schnelle Umsetzung der Richtlinie nur eine Anpassung auf niedrigem Niveau bringen; die Chance einer grundsätzlichen Neuorientierung wäre vertan. Es muss sich zeigen, ob die Initiativen der neuen Bundesregierung nunmehr eine andere Situation schaffen; in diesem Fall sollte der Landesgesetzgeber ebenfalls aktiv werden, wenn auch angesichts des Ablaufs der Legislaturperiode in diesem Herbst realistischerweise eine parlamentarische Behandlung im Jahre 1999 nicht mehr möglich sein dürfte.

In der Berliner Verwaltung ist neben der Haushaltssanierung die *Verwaltungsreform* das beherrschende Thema. Ihre Durchsetzung bedarf einer Vielzahl von Gesetzesänderungen im Detail, die auch datenschutzrechtliche Aspekte aufweisen. Im vergangenen Jahr wurde das 2. Verwaltungsreformgesetz[34] verabschiedet, das neue Formen des Informationsaustauschs zwischen den Ordnungsbehörden vorsieht.

Nicht vorangekommen sind die Beratungen über ein Berliner *Informationsfreiheitsgesetz,* das von der Fraktion Bündnis 90/Die Grünen eingebracht wurde[35]. Nachdem das Land Brandenburg als erstes Bundesland über ein derartiges Gesetz verfügt[36], wäre es ein Beleg für die Aufgeschlossenheit der Bundeshauptstadt, wenn diese, einem weltweiten Trend folgend, ebenfalls den Zugang zu den Akten der öffentlichen Verwaltung ohne individuelle Voraussetzungen ermöglichen würde. Dass dies ohne unangemessene Beeinträchtigung des Datenschutzes geschehen kann, hat nicht nur Brandenburg bewiesen, sondern ist von der Konferenz der Datenschutzbeauftragten auch ausdrücklich bestätigt worden[37].

Die Meinungsverschiedenheiten über die Befugnis der Sozialleistungsträger, den Sicherheitsbehörden, vor allem aber der Ausländerbehörde, den *künftigen Aufenthaltsort von Sozialleistungsempfängern* mitzuteilen *(„Sozialamtsfalle“),* hielten an[38]. Zwar hat der Bundesgesetzgeber nunmehr eine entsprechende Befugnis im *Sozialgesetzbuch* geschaffen[39], diese ist aber an Voraussetzungen geknüpft, die gleichwohl eine

32 4. StUÄndG vom 19. 12. 1998 BGBl. I S. 3778
33 Drittes Änderungsgesetz zum Hessischen Datenschutzgesetz v. 5. 11. 1998, GVBl. S. 421 ff.; Zweites Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes v. 21. 12. 1998, BGBl. S. 243
34 Zweites Gesetz zur Reform der Berliner Verwaltung v. 25. Juni 1998, GVBl. S. 177
35 Abghs.-Drs. 13/1623
36 Akteneinsichts- und Informationszugangsgesetz v. 10. 3. 1998, GVBl. I S. 46
37 JB 1997, Anlage 2.3.4
38 vgl. JB 1997, 3.1, 3.2
39 vgl. oben und 4.4.3

Änderung der bestehenden, von uns für rechtswidrig gehaltenen Berliner Verwaltungsvorschriften erforderlich machen. Während die Sozialverwaltung die Bestimmungen für die Weitergabe von Daten an die Sicherheitsbehörden, insbesondere im Fahndungsfall, an die Rechtslage anpasste, weigert sich die Innenverwaltung nach wie vor, dasselbe für die Weitergabe an Ausländerbehörden zu tun[40].

Im Übrigen sind keine wesentlichen Änderungen des Berliner Datenschutzrechts eingetreten. Dies ist sicherlich darauf zurückzuführen, dass auf der Grundlage des relativ strengen Berliner Datenschutzgesetzes in den vergangen Jahren der Datenschutz eine hinreichende, wenn auch nicht immer im Sinne der Bürger zufrieden stellende Rechtslage geschaffen wurde.

2. Technische Rahmenbedingungen

2.1 Die Entwicklung der Informationstechnik

Die Trends

Die alljährlich an dieser Stelle beschriebenen Entwicklungstendenzen in der Informationstechnik sind ungebrochen. Wenn also etwas unverändert ist, dann ist es der Trend zu informationstechnischen Systemen mit immer günstigerem Preis-Leistungs-Verhältnis und zum Zusammenwachsen von Kommunikations- und Informationstechnik und der damit zusammenhängenden Vernetzung.

Immer noch werden die Prozessoren schneller, der verfügbare Raum im Arbeitsspeicher und in den Festplatten wird immer größer und es kommen weitere externe Speichermedien mit immer größeren Kapazitäten auf den Markt.

Die Entwicklung belegt eine Tabelle, die eine pauschalisierte Darstellung der vorweihnachtlichen Angebote für häusliche Komplettsysteme der gehobene Leistungsklasse der letzten vier Jahre enthält:

Jahr	Prozessortakt	Arbeitsspeicher	Festplatte	CD-ROM
1995	100 MHz	16 MB	1,0 GB	4-fach
1996	200 MHz	32 MB	1,5 GB	12-fach
1997	300 MHz	32 MB	6,0 GB	24-fach
1998	400 MHz	64 MB	12,0 GB	40-fach

Einschließlich der aktuellen Versionen der gängigen Betriebs- und Bürosoftware sowie der notwendigen Peripherie nach dem jeweiligen Stand der Technik haben die Preise trotz der verbesserten Leistungsdaten noch weiter nachgelassen.

[40] vgl. 4.4.3

Da die durch die Geschwindigkeit und die Speicherkapazitäten gesetzten Grenzen immer weiter hinausgeschoben werden, kann auch die Software, insbesondere die Standardsoftware, immer komplexer werden. Die gewonnenen Ressourcen werden im Wesentlichen für drei Zielsetzungen genutzt:

- Der Mensch-Maschine-Dialog wird durch die Verbesserung der *graphischen Schnittstellen* und der Aufbereitung der *Oberfläche* optimiert. Dies kommt insbesondere bei den Computern zur privaten Nutzung zur Geltung, weil gerade Computerspiele und Internetangebote durch immer raffiniertere Gestaltung die Ansprüche des verwöhnten Publikums befriedigen wollen. Im kommerziellen Bereich bieten sich Chancen für die ergonomische Schnittstellengestaltung und natürlich für graphisch orientierte Spezialanwendungen.
- Bei kommerziellen Anwendungen entfernen sich die für die Benutzer bereitgestellten Methoden der Datenauswertung immer mehr von der Erfordernis der Datenstrukturierung. Beispiele dafür sind *Volltextretrievalsysteme* sowie *Datamining-Techniken* zur Erschließung von *Data-Warehouses*[41].
- Bei den Anwendungen in Wirtschaft und Verwaltung kommt es zur verstärkten Verlagerung des gesamten Informationswesens auf die informationstechnischen Systeme. Aktenarchive werden digital archiviert und so „entstaubt". Integrierte Systeme wie z. B. die *kommerziellen Standardprogrammsysteme* wie R/3 des deutschen Softwareunternehmens SAP unterstützen die organisatorische Steuerung[42].

Die Vernetzung informationstechnischer Infrastrukturen geht einher mit dem Zusammenwachsen von Informations-, Telekommunikations- und Televisionstechnik. Das Internet transportiert Daten, Sprache, Bilder, Fernsehübertragungen und Videofilme, also alles, was sich mit digitalen Zeichenfolgen darstellen, übertragen und verarbeiten lässt.

Die aktuellen Beiträge zur Entwicklung der Informationsgesellschaft

Angesichts dieser ungebrochenen Trends fragt es sich, welche Bedeutung sie für den Einstieg in die Informationsgesellschaft haben. Welche Erwartungen, Hoffnungen oder Befürchtungen werden damit verbunden?

Die Entwicklung der Informationstechnik kann nicht nur an den sich zum Besseren verändernden Leistungsmerkmalen gemessen werden. Was sich in der Informationstechnik durchsetzt, wird nicht nur durch anerkannte Qualitätsstandards bestimmt, häufig ist es die Stellung der

[41] vgl. JB 1997, 2.1
[42] siehe 4.8.1

Hersteller im Markt, sind es unkonventionelle Methoden der Markteinführung. Häufig sind es die klassischen Flaschenhalseffekte, die neuen und besseren Produkten die Markteinführung erschweren: Solange ihre Kompatibilität mit eingeführten Standardprodukten nicht gesichert ist, solange nicht genügend Software verhanden ist, die mit abweichenden Produkten arbeitet, solange passende Schnittstellen nicht in Standardsystemen berücksichtigt werden, haben es neue Technologiekonzepte schwer, sich durchzusetzen, bevor sie selbst veraltet sind. Dies gilt z. B. für die DVD-Speichermedien (Digital Versatile Disk), die der CD-ROM weit überlegen ist, dennoch nur zögerlich angenommen werden.

Die Verbreitung des *Internet* zeigt, dass dieses die Bottleneck-Phase überwunden hat. Die Zahl der Netzsurfer steigt Tag für Tag, ständige Meldungen über Firmengründungen für Dienstleistungen im Internet zeigen, dass große Erwartungen zur Zukunft des elektronischen Handels und der elektronischen Präsentation im Internet gehegt werden. Allerdings wird die Internet-Euphorie bereits durch einige bittere Erkenntnisse abgekühlt: Die öffentliche Meinung über das Internet wird insbesondere bei jenen, die keine besonderen Anwendererfahrungen mit dem Netz haben, durch Schlagzeilen bestimmt, die den Missbrauch des Netzes zur Verbreitung gesetzwidriger oder unerwünschter Inhalte betreffen. Ähnlich wie das gute alte Bildschirmtextsystem zieht auch das Internet offensichtlich die Anbieter von kriminellen Pornographievarianten, von Gewaltverherrlichung und politischer Bauernfängerpropaganda an. Damit wird auch jenen in die Hand gearbeitet, die Informations- und Kommunikationsfreiheit nur als eine Gefahr für die öffentliche Sicherheit und Ordnung sehen und entsprechende Kontrollstrukturen fordern und durchzusetzen versuchen.

Weitere Ernüchterung kommt bei dem auf, der der Werbung der Internet-Provider erlegen ist und als Privatmensch in die weite Welt hinaussurfen möchte. Die Kapazität des Internet und der in ihm operierenden Komponenten vom anbietenden Server über die Übertragungsleitungen, die weiterleitenden Rechner auf dem Übertragungsweg, den eigenen Netzanschluss und den eigenen Rechner sind dem anstehenden Datenstrom nicht mehr immer so gewachsen, dass Antwortzeiten erreicht werden, die die Kommunikationskosten als angemessen erscheinen lassen. Der von allen erwartete weitere Innovationsschub, der uns der Informationsgesellschaft näher bringt, wird die Erweiterung der *Netzkapazitäten* erforderlich machen. Erste Pilotprojekte – z. B. der Bewag in Berlin[43] befassen sich mit der Nutzung der Netze zur allgemeinen Stromversorgung als Datenübertragungsmedien.

[43] Projekt „Düne" – Datenübertragung über Niedrigspannungs-Energienetze – dazu gibt es diverse Pressemeldungen, z. B. Berliner Zeitung v. 24. 7. 1998, S. 26: „Telefonieren und Faxen per Stromleitung"; Computer Zeitung v. 13. 8. 1998, S. 16: „Über die digitale Powerline erhält der PC aus der Steckdose außer Strom auch Daten"; Der Tagesspiegel v. 6. 9. 1998: „Bewag bereitet Revolution in der Fernsprechtechnik vor"

Tops und Flops auf dem Weg in die Informationsgesellschaft

Während niemand auf die Idee käme, trotz der euphoriedämpfenden Beobachtungen Zweifel an der Bedeutung des Internet für die Informationsgesellschaft zu hegen, zeigt eine Rückbesinnung auf technologische Trends, die in den letzten Jahren an dieser Stelle dargestellt wurden, dass manches, was den Sonnenaufgang der Informationsgesellschaft ankündigte, wohl mehr eine Sternschnuppe war:

1991 befassten wir uns erstmals mit den „Trends der informationstechnischen Entwicklung" und beschrieben, wie danach alle Jahre, die heute noch gültigen Haupttendenzen zur Verbesserung des Preis-Leistungs-Verhältnisses, die Miniaturisierung und die Vernetzung. Die erwähnte Zusammenführung der Rechnernetze zu einem *„Global Area Network* (GAN)" ist mit dem Internet heute ebenso Realität geworden wie die Durchsetzung objektorientierter Programmierung, mit der die neuen Leistungskapazitäten softwareseitig erschlossen werden können[44].

1992 berichteten wir über *Downsizing* und *Outsourcing* als aktuelle Trends des IT-Einsatzes. Beides ist heute selbstverständlich, die dreidimensionale computergesteuerte Scheinwelt des „Cyberspace" jedoch, in der sich die Menschen mit Datenhandschuhen, Datenbrillen und Datenanzügen bewegen, ist ein Nischenprodukt geblieben[45].

Im darauf folgenden Jahr befassten wir uns erstmals mit *Chipkarten,* die z. B. als Krankenversichertenkarten im Jahre 1994 an breite Teile der Bevölkerung verteilt wurden[46]. Wir haben keine Zweifel, dass Chipkarten in der Zukunft in verschiedensten Anwendungen eine bedeutsame Rolle spielen werden. Allerdings zeigt sich eine große Differenz zwischen dem Engagement, mit dem Kartenhersteller und potenzielle Anwender den Einsatz der Chipkartentechnik vorantreiben wollten, und dem Interesse der Bevölkerung. Als erfolgreich können bisher nur solche Chipkarteneinführungen angesehen werden, die primitive anonyme Zahlungsverfahren anbieten (Telefonkarte) oder die dem Verbraucher aufgezwungen wurden, wie die Krankenversichertenkarten. Weitere Projekte, insbesondere im Gesundheitswesen und im Zahlungsverkehr[47], haben über den Erprobungsbereich hinaus keine besondere Bedeutung erlangt oder sind sogar gescheitert.

1994 wurden das *Internet, Client-Server-Systeme* und *optische Speichermedien* behandelt, Technologien also, deren erfolgreiche Durchsetzung bereits damals unschwer vorherzusagen war[48].

[44] JB 1991, 1.2
[45] JB 1992, 2.1 und 2.3
[46] JB 1993, 2.3
[47] insb. JB 1995, 3.2
[48] JB 1994, 2.1

Danach wurde die *Einführung von WINDOWS 95* zum Gegenstand der Trendbeschreibung gemacht, was sicher für den semiprofessionellen und privaten Sektor angebracht war, während sich in den Client-Server-Netzen der kommerziellen Computeranwender WINDOWS NT stärker durchsetzen konnte[49]. Die damals beschriebenen Sicherheitsprobleme im Zusammenhang mit dem Microsoft Network (MSN) haben in Deutschland nicht die Bedeutung erlangt, weil MSN keine große Verbreitung in unserem Lande gewonnen hat[50].

Im Vorjahr beschrieben wir die Entwicklung von Client-Server-Systemen zu *Network Computing* und das Schürfen in (Daten-)Banken und (Daten-)Warenhäusern mit modernen Methoden des *Data Mining*[51]. Während der letztere Trend gerade durch die Verbesserung des Preis-Leistungs-Verhältnisses noch zusätzlichen Rückenwind bekommen hat, müssen wir auf den Siegeszug der *Netzwerkcomputer,* der Steckdosen zu Intranet und Internet, noch warten. Hier ist ein marktwirtschaftlicher Prozess im Gange, dessen Ergebnis noch nicht vorhergesagt werden kann.

Wer ist in der Informationsgesellschaft informiert?

Im Berichtsjahr fand sich kein besonders hervorzuhebener technologischer Trend, der uns das Bild von der zukünftigen Informationsgesellschaft klarer machen könnte. Eine politisch motivierte Entwicklung mag jedoch zu denken geben, die sich aus vielen nationalen und internationalen rechtspolitischen Diskussionen und aktuellen Veröffentlichungen ergeben hat. Das folgende erdachte, aber auf konkreten technologischen Ansätzen beruhende Szenario möge so zu denken geben, dass es zumindest so nie Wirklichkeit werden möge:

„Wie jeden Sonntag trabt ein einsamer Jogger durch den nebelfeuchten Grunewald, um den Stress verantwortlicher Arbeit aus der letzten Woche abzuschütteln. Nach einigen Kilometern wird ihm klar, dass er sich etwas zu viel zumutet, und trottet auf eine Parkbank zu, um das Sauerstoffdefizit bei einer kleinen Pause aufzufrischen. Er merkt nicht, dass er inzwischen anderswo hektische Aktivitäten auslöst, die sich bald auch auf weite Teile der Welt ausdehnen sollen.

49 JB 1995, 2.1

50 Auf die Bewertung von WINDOWS 98 als erwähnenswerter neuer technologischer Trend wollen wir zumindest diesmal verzichten, da der Innovationsgrad in der Fachwelt noch umstritten ist. Ebenso wollen wir das erfolgreiche Comeback von Apple hier erwähnen und abwarten, ob sich hier ein Trend gegen die Microsoft-beherrschte Welt abzeichnet.

51 JB 1997, 2.1

Ein kleiner, unter die Haut transplantierter Transponderchip[52]*, den er wie die anderen leitenden Biochemiker der gentechnischen Entwicklungsabteilung seines Berliner Hightech-Unternehmens trägt, hat nämlich Abweichungen von den üblichen Kreislaufwerten festgestellt, die die Gefahr eines Herzinfarktes andeuten. Über ein miniaturisiertes Empfangsgerät seines in der Sportkleidung integrierten Personal Area Networks*[53] *wird der Alarm mit einigen spezifizierenden, lokalisierenden*[54] *und identifizierenden Angaben über das mitgeführte Mobiltelefon automatisch an die Alarmbereitschaft des Unternehmens weitergeleitet. Diese setzt den Notarzt in Marsch, während unser matter Jogger noch glaubt, sich nur ein paar Minuten ausruhen zu müssen. Als er merkt, dass es ihm schlechter geht als üblich nach einem anstrengenden Lauf, setzt der Rettungshubschrauber bereits auf der benachbarten Waldlichtung auf.*

Dies wäre das Ende der Geschichte einer schnellen geglückten Rettung, bevor sich der Verschluss der Herzkranzgefäße erst richtig auswirken könnte. Doch moderne Informations- und Kommunikationstechnik leistet mehr:

Das automatisch ausgelöste digitale Mobiltelefonat zur Alarmbereitschaft des Hightech-Unternehmens enthält mit den Identifikatoren des Patienten und des Unternehmens Schlüsselworte, die die Computer des Nachrichtendienstes eines befreundeten Staates bei der Analyse des mit Hilfe des globalen Telekommunikationsüberwachungssystems ECHELON aufgezeichneten Mobiltelefonverkehrs in Berlin dazu veranlassen, das Gespräch zu selektieren und zur weiteren geheimdienstlichen Auswertung bereitzustellen[55]*.*

Die Information, dass ein leitender Entwickler in der Genforschung eines erfolgreichen Berliner Unternehmens durch einen Herzinfarkt außer Gefecht gesetzt worden ist, erreicht bereits nach wenigen

52 Die Welt vom 19. 1. 1998 „Der Chip ruft im Notfall den Arzt“ und die ComputerBild 5/98 „Rettungs-Einsatz“ berichteten über das „Implementierbare Telemetrische Endosystem – ITES“, welches in einem Bremer Forschungsinstitut in Zusammenarbeit mit neun anderen Instituten entwickelt worden ist und aus dem Körper eines Patienten verschiedenste Messwerte nach außen senden kann

53 Die Computer Zeitung vom 2. 7. 1998 meldete auf S. 26, dass das IBM-Forschungszentrum in San Jose an der Technologie von Personal Area Networks (PAN) arbeitet, denen der menschliche Körper als Transportmedium elektrischer Signale dient und die auf Signale reagieren, die vom Menschen ausgehen (z. B. Gesichtsausdrücke, Gefühlsregungen – warum dann nicht auch Messwerte?)

54 Hier hilft der mitgeführte GPS-Sender (Global Positioning System), mit dem der genaue Aufenthaltsort satellitengestützt festgestellt werden kann, siehe z. B. JB 1995, 3.3, im Zusammenhang mit der Positionsbestimmung von fahrenden Kraftfahrzeugen zur Erhebung der elektronischen Maut

55 Der Tagesspiegel berichtete am 26. 9. 1998 auf S. 2 unter der Überschrift „Totale Kontrolle der Bürger durch ‚elektronische Fangnetze‘“ über den Bericht an den Ausschuss für Grundfreiheiten des Europaparlaments und das Straßburger Gremium zur Technologienbewertung – STOA – über „eine Bewertung der Technologien für eine politische Kontrolle“ vom September 1998, im Internet als Zusammenfassung veröffentlicht unter http://www.europarl.eu.int/dg4/stoa/de/publi/166499/execsum.htm. Hierin wird berichtet, dass mit ECHOLON alle E-Mail-, Telefon- und Faxverbindungen nichtmilitärischer Zielgruppen in Europa routinemäßig vom US-Geheimdienst NSA angezapft werden

Stunden das Management des größten Konkurrenzunternehmens in dem befreundeten Staat, so dass geprüft werden kann, wie dieses Ereignis zu eigenen Gunsten ausgewertet werden kann."

Dieser fiktive Fall zeigt die Bedeutung, die die Sicherstellung der Vertraulichkeit für die Telekommunikation künftig haben wird. Das entscheidende Mittel hierfür ist die Verschlüsselung der Nachrichten.

1998 war ein Jahr, in dem international heftig in der Kryptokontroverse gestritten wurde[56]. Insbesondere die US-Regierung hat verstärkten diplomatischen Druck – vor allem durch Entsendung eines sog. „Krypto-Sonderbotschafters" – auf die verbündeten Staaten ausgeübt, starke kryptografische Verfahren zur Verschlüsselung der Sprach- und Datenkommunikation in internationalen Kommunikationsnetzen, insbesondere dem Internet, nur unter der Bedingung zuzulassen, dass die Schlüssel – möglichst bei amerikanischen Sicherheitsbehörden – hinterlegt oder rekonstruierbar gemacht werden. Diese Forderung wurde im sog. Wassenaar-Abkommen vom 3. 12. 1998, dem auch die Bundesregierung zusammen mit 32 weiteren Staaten zugestimmt hat, nicht durchgesetzt. Allerdings wurde der Export leistungsfähiger Verschlüsselungsprodukte mit einer Schlüssellänge von mehr als 64 bit einer Genehmigungspflicht unterworfen[57].

Verfolgt man diese Entwicklung auch im Lichte der aktuellen rechtlichen Entwicklung, die die Kontrolle der Telekommunikation in Deutschland und Europa betrifft[58], so ist 1998 folgender Trend dann doch besonders aufgefallen: Der anarchischen Entwicklung des Internet in den letzten Jahren werden jetzt die Strukturen aufgedrückt, die es der über- und innerstaatlichen Überwachung aussetzen sollen: Globale Überwachung für globale Infrastrukturen. Ob dies die Informationsgesellschaft verträgt, bleibt abzuwarten und darf bezweifelt werden.

2.2 Datenverarbeitung in Berlin

Die Organisation der Datenverarbeitung in der öffentlichen Verwaltung Berlins

Wesentlicher Bestandteil der Berliner Verwaltungsreform ist der effiziente Einsatz moderner Informationstechnik zur Straffung von Verwaltungsabläufen, zur Personaleinsparung, zur Modernisierung der Arbeitsumgebungen und insbesondere zur Verbesserung des Dienstes am Bürger durch schnellere Bedienung, Vermeidung zusätzlicher Behördenwege und Verbesserung der Beratungsmöglichkeiten.

56 JB 1996, 3.4
57 C. Schulzki-Haddouti: Keine Krypto-Verschwörung, c't 1998, Heft 22, S. 32 f. und dies.: Umrüstung – Kryptographie gilt weiterhin als Waffe, c't 1998, Heft 26, S. 52 f.
58 vgl. 5.2

Diese ehrgeizigen Ziele sind nicht nur mit der Bereitstellung von Mitteln für die Beschaffung von Informationstechnik zu erreichen. Es musste auch der Wildwuchs ausgebremst werden, der sich in einigen Jahren ergeben hatte, in denen IT-Einsatz nur sehr zurückhaltend koordiniert wurde. Unter der Leitung eines Referats der Service-Abteilung der Senatsverwaltung für Inneres wurde ein *IT-Koordinations- und Beratungsausschuss* (IT-KAB) eingerichtet[59], in dem die IT-Manager der Hauptverwaltung und Bezirke in paritätischer Zusammensetzung vertreten sind. Dieser IT-KAB hat die wesentlichen übergreifenden Koordinationsaufgaben übernommen. Besonders hervorzuheben sind zwei Ergebnisse dieser Arbeit: Die IT-Organisationsrichtlinie und die IT-Sicherheitsrichtlinie.

Die *IT-Organisationsrichtlinie* wurde am 17. März 1998 vom Senat verabschiedet. Ihr Ziel ist die Festlegung organisatorischer Grundstrukturen durch die Definition unterschiedlicher dezentraler und zentraler Rollen bei der Planung, Gestaltung und Nutzung von IT-Anwendungen und -Infrastrukturen sowie die Beschreibung der Art und Weise, mit der die Träger der Rollen miteinander in Beziehung treten.

Die *IT-Sicherheitsrichtlinie* stand Ende des Jahres erst vor der abschließenden Behandlung im Senat, soll aber nach einem Beschluss des IT-KAB bereits jetzt angewendet werden. Da sie für die IT-Sicherheit und damit auch für den technisch-organisatorischen Datenschutz von zentraler Bedeutung ist, soll sie hier etwas ausführlicher dargestellt werden.

In den Grundsätzen der IT-Sicherheitspolitik des Landes wird betont, dass alle Aspekte der IT-Sicherheit unabdingbare Voraussetzung und Bestandteil jedes IT-Einsatzes während des gesamten Einsatzzeitraumes zu sein und dass dafür Sicherheitskonzepte zu bestehen haben. Die notwendigen Maßnahmen sind auch dann zu ergreifen, wenn sie den IT-Einsatz erschweren. Wenn die notwendige Sicherheit nicht gewährleistet werden kann, ist auf den IT-Einsatz zu verzichten. Die Sicherheitsmaßnahmen haben einer ständigen Qualitätskontrolle zu unterliegen.

Der *Landesbetrieb für Informationstechnik* (LIT) hat als zentraler Infrastrukturbetreiber bestimmte Sicherheitsdienstleistungen (Verschlüsselung, Grenznetz zum Internet) im Berliner Landesnetz anzubieten, die als Pflichtdienste von den Stellen zu nutzen sind, die die zentrale IT-Infrastruktur (Landesnetz, Sicherheitsrechenzentrum, Intranet) nutzen wollen. Wenn eine Behörde die notwendige Sicherheit nicht gewährleisten kann oder will, kann der LIT die Dienstnutzung verweigern.

59 JB 1997, 2.3

Das Prinzip des Vorrangs datenschutzfreundlicher Technologien, in denen die Identität der Personen durch Anonymisierung oder Pseudonymisierung geschützt werden kann[60], ist in der IT-Sicherheitsrichtlinie berücksichtigt worden.

Die in der *IT-Organisationsrichtlinie* definierten Rollen bei der Erarbeitung zentraler oder dezentraler, anwendungs- oder infrastrukturbezogener Sicherheitskonzepte, ihrer Umsetzung und Beachtung sowie ihrer Kontrolle sind unmissverständlich bestimmt worden.

Das methodische Vorgehen hat sich am *IT-Grundschutzhandbuch* des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[61], bei erhöhtem Schutzbedarf partiell oder vollständig am IT-Sicherheitshandbuch des BSI zu orientieren[62]. Dies bedeutet, dass die Sicherheitskonzepte die Risiken abzudecken haben, die in einzelfallbezogenen Risikoanalysen oder -betrachtungen ermittelt worden sind.

Der IT-KAB hat eine ständige Arbeitsgruppe „IT-Sicherheit“ unter der Federführung der Senatsverwaltung für Inneres und unter beratender Beteiligung des Rechnungshofs von Berlin und des Berliner Datenschutzbeauftragten eingerichtet, die einen regelmäßigen Informations- und Erfahrungsaustausch gewährleistet, einen jährlichen Sicherheitsbericht erarbeitet und einen jährlichen Umsetzungsplan IT-Sicherheit für die Beschlussfassung im IT-KAB vorbereitet.

In einer Anlage zur IT-Sicherheitsrichtlinie wurden *Sicherheitsstandards* vorgegeben. Sie heben den besonderen Schutzbedarf personenbezogener Daten hervor und verlangen die Einrichtung von Trust-Centern für die digitale Signatur, von gestaffelten Firewalls beim Anschluss von Sicherheitsdomänen an das Berliner Landesnetz, von geschlossenen Benutzergruppen zur gegenseitigen Abschottung von Verfahren, die Verschlüsselung schutzbedürftiger Daten bei Übertragung und Transport, ggf. auch der Speicherung.

Insgesamt ist festzustellen, dass die Umsetzung der IT-Sicherheitsrichtlinie eine wesentliche Verbesserung der Sicherheit des IT-Einsatzes im Lande sowie deren Kontrolle ermöglichen wird. Voraussetzung dafür ist, dass die Richtlinie nicht nur ein Papiertiger bleibt. Dies dürfte nur dann erreicht werden, wenn sich auch bei den Verantwortlichen für den lokalen Einsatz der Informationstechnik ein Sicherheitsbewusstsein entwickelt und festigt. Solange Sicherheitsmängel aus Gründen der Bequemlichkeit oder wegen falscher Prioritätensetzungen hingenommen werden, ist Skepsis angebracht.

60 siehe JB 1997, 2.2

61 Bundesamt für die Sicherheit in der Informationstechnik (BSI): IT-Grundschutzhandbuch – Maßnahmenempfehlungen für den mittleren Schutzbedarf, Bundesanzeiger Verlagsges., Köln 1998

62 Bundesamt für die Sicherheit in der Informationstechnik (BSI): IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, Vs. 1.0 – März 1992, Eigenverlag, Bonn

Berliner Landesnetz – MAN

Im Jahresbericht 1997[63] bedauerten wir, dass im Zusammenhang mit der Änderung der Rechtsform des LIT der bis dahin gut funktionierende Informationsfluss zu sicherheitstechnischen Fragestellungen in signifikanter Weise unterbrochen wurde, da der im Jahre 1996 ins Leben gerufene Arbeitskreis „Netzsicherheit“ im LIT, der einen koordinierten Informationsaustausch im Bereich der Netzsicherheit im gesamten Berliner Landesnetz erreichen sollte, leider aufgelöst wurde. Dieser für die Verbesserung der Sicherheit im Berliner Landesnetz so wichtige Informationsaustausch wurde nunmehr durch Einsetzen einer Arbeitsgruppe „IT-Sicherheit“ (s. o.) durch den IT-KAB – unter Federführung der Senatsverwaltung für Inneres – wieder belebt.

Die Tendenz des letzten Jahres – Pläne zur *Anbindung an das Internet* und zur damit verbundenen Nutzung von Internet-Diensten durch die Verwaltung – setzte sich fort. Grundlage für die Internet-Anbindung des Berliner Landesnetzes ist das *Grenznetz* im LIT. Ein zentrales *Firewall-System* bildet das Kernstück des Grenznetzes. Dieses soll den gesicherten Übergang zwischen dem MAN und dem Internet realisieren. Ergänzt wird das zentrale Firewall-System durch dezentrale Systeme in den jeweiligen Subnetzen der Bezirks-, Senats- und sonstigen Verwaltungen, die zusammen ein gestaffeltes Firewall-System bilden[64].

Zu den dezentralen Komponenten in den Subnetzen gehören verschiedene *Proxy-Server,* die insbesondere die Authentifikation der berechtigten Nutzer der Internet-Dienste gewährleisten. Eine wesentliche Aufgabe von Firewall-Systemen ist die Protokollierung von sicherheitsrelevanten Ereignissen. Hierbei mussten wir feststellen, dass es recht unterschiedliche Auffassungen vom Begriff der sicherheitsrelevanten Ereignisse und vom Umfang und der Aufbewahrungsdauer der Protokolle gibt.

Generell lässt sich feststellen, dass beim Betrieb einer Firewall jede Protokollierung so ausgestaltet sein sollte, dass unter Wahrung des Zwecks ein datenschutzrechtlicher Missbrauch vermieden wird, d. h.:

- der Umfang der Protokolle sollte im Rahmen des Möglichen minimal sein,
- Protokolle sind durch Zugriffsmaßnahmen gegen unbefugte Kenntnisnahme zu sichern,
- es sind technisch-organisatorische Auswertungsverfahren festzulegen und
- es sind möglichst kurze Löschungsfristen vorzusehen.

63 JB 1997, 2.3

64 JB 1995, 4.1 und JB 1997, 2.3

Das Stadtinformationssystem (SIS), der Weg in die interaktive Verwaltung?

Das Land Berlin präsentiert sich seit Dezember 1998 mit einem elektronischen *Stadtinformationssystem* (SIS) im Internet[65]. Das SIS soll die Bürgerinnen und Bürger der Stadt, die in der Region ansässigen Wirtschaftsunternehmen, öffentliche und private Einrichtungen, die Berlin-Besucher und an Berlin Interessierte weltweit unter Nutzung elektronischer Medien über alle Angelegenheiten der Stadt und ihrer verschiedenen Lebensbereiche informieren. Vorläufer des SIS war die „Informations-Datenbank Berlin“ mit über 16 000 Bildschirmtext-Seiten[66].

Durch diesen weiteren Schritt in die Nutzung neuer Medien und damit in eine neue Generation der Informationsdarstellung und des Informationsabrufs werden für die Benutzer auch qualitativ neue Dienstleistungen der Verwaltung möglich. So soll das SIS kein reines Informationssystem im herkömmlichen Sinne sein. Vielmehr sollen durch die Einführung interaktiver Verwaltungs- und Serviceanwendungen im Kontakt zwischen der Öffentlichkeit und Verwaltung sowie kommerzieller Anbieter neue Kommunikationsstrukturen entwickelt werden. Durch die Vereinfachung des Zugangs zu Verwaltung und Verwaltungsabläufen sowie durch die damit erhoffte Beschleunigung des Verwaltungshandelns soll mehr Bürgernähe erreicht werden – eines der wichtigsten Ziele der Verwaltungsreform.

Das SIS wird sich nicht nur an die Internet-Teilnehmer richten. Es ist vorgesehen, mehrere Hundert Infosäulen *(Kiosksysteme)* an öffentlich zugänglichen Plätzen, wie z. B. Flughäfen oder Rathäuser, über die Stadt zu verteilen, um damit den Zugang für jeden Bürger zu ermöglichen.

Die Planungen für interaktive Verwaltungsdienstleistungen reichen von der Anmeldung zu Volkshochschulkursen über die Beantragung von Wohngeld bis hin zur melderechtlichen An-, Um- oder Abmeldung und der Einsicht in das Melderegister. Auch die Anmeldung eines gekauften PKW, sogar die Abgabe der Steuererklärung oder der Abruf von Kataster- und Grundbuchauszügen werden als interaktive Dienstleistungen nicht ausgeschlossen.

Doch diese Neuerungen stehen unter dem Vorbehalt, dass die entstehenden Sicherheitsprobleme gelöst werden:

– So ist sicherzustellen, dass der elektronische *Wohngeldantrag* auf dem Kommunikationsweg nicht von Unbefugten mitgelesen oder gar verfälscht werden kann. Die Vertraulichkeit und Integrität der elektronischen Kommunikation zwischen Bürger und Verwaltung ist zu gewährleisten.

[65] http://www.berlin.de
[66] * Berlin #

– Die Wohngeldstelle muss sicher sein, dass der Wohngeldantrag auch wirklich von der Person stammt, die als Absender auf dem elektronischen Antrag steht. Die Authentität der Kommunikationspartner ist also zu gewährleisten.

– In manchen Fällen ist eine Auskunft aus öffentlichen Registern an die Geltendmachung eines *berechtigten Interesses* gebunden. Es ist also ein Weg zu finden, wie dieses über die Internet-Kommunikation erreicht werden kann.

– Die Öffnung von Verwaltungsverfahren und -registern für Bürger über das Internet kann *Hacker* auf den Plan rufen, die versuchen könnten, die allen Bürgern eingeräumten Zugriffsrechte zu erweitern und missbräuchlich zu nutzen.

Mit der Abwicklung solcher Verwaltungsabläufe über elektronische Medien werden also zahlreiche datenschutzrelevante und sicherheitstechnische Fragestellungen aufgeworfen. Aus Datenschutzsicht sind daher folgende Anforderungen zu formulieren:

– Da die geltenden *Rechts- und Verwaltungsvorschriften* noch nicht auf die Anforderungen einer Kommunikation über neue Medien zugeschnitten sind, müssten diese daher verändert oder neu erlassen werden, um interaktive Verwaltungsdienstleistungen zu ermöglichen.

– Zur Sicherstellung der Vertraulichkeit sind bei der Übertragung personenbezogener Daten im Rahmen von Verwaltungsdienstleistungen sichere *Verschlüsselungsverfahren* anzuwenden.

– Zur Sicherstellung der Integrität und der Authentität der Kommunikation und Kommunikationspartner müssen Verfahren zur *elektronischen Unterschrift* nach Vorgaben des Signaturgesetzes eingeführt werden. Die notwendigen Trust-Center bzw. Zertifizierungsstellen müssen aufgebaut und in Betrieb genommen werden.

– Die beteiligten Systeme der Verwaltung sind mit *Firewallsystemen* gegen von außen kommende Sicherheitsrisiken abzuschotten.

– Die *Protokollierung* von Bürgeraktivitäten bei der Inanspruchnahme interaktiver Verwaltungsdienstleistungen hat – sofern sie überhaupt erfolgen muss – der engen Zweckbindung nach § 11 Abs. 5 BlnDSG zu genügen und darf nicht zu anderen Zwecken ausgewertet werden.

– Sofern *Registerabfragen,* die ein berechtigtes Interesse voraussetzen, interaktiv erfolgen sollen, sind Verfahren zu konzipieren, die das berechtigte Interesse plausibel machen können (z. B. elektronisch zu unterschreibende Erklärungen bzw. Erläuterungen). Für Personengruppen, für die ein berechtigtes Interesse bei bestimmten interaktiv erreichbaren Registern von vornherein angenommen

wird (z. B. Notare), sind geschlossene Benutzergruppen vorzusehen, deren Mitglieder einer dem Stand der Technik entsprechenden Authentifizierung unterliegen müssen.

Das Stadtinformationssystem wird im Rahmen eines *Public-Private-Partnership* in Kooperation mit einem kommerziellen Dienstleister realisiert. Die technische Plattform wird vollständig vom Dienstleister zur Verfügung gestellt und soll allein durch Werbung finanziert werden. Ob diese enge Zusammenführung kommerzieller Interessen einerseits und der Verwaltungsabläufe andererseits datenschutzrechtliche Relevanz erhält, wird in der Praxis sorgfältig zu beobachten sein.

Neben den geplanten interaktiven Verwaltungsdienstleistungen werden den Benutzern zahlreiche Informationen der verschiedenen Verwaltungen der Stadt, wie z. B. Öffnungszeiten und Ansprechpartner, zur Verfügung gestellt. Diese Informationen sind zentral auf dem Server des Stadtinformationssystems gespeichert, werden jedoch von den einzelnen Verwaltungen selbständig erstellt und aktualisiert. Für die dezentrale Pflege der Informationen wurde ein Redaktionswerkzeug auf Basis von Standard-Internet-Browsern realisiert. Dieses Redaktionswerkzeug kann einerseits über das Internet und andererseits über eine Modem-Einwahl beim Betreiber der technischen Plattform genutzt werden. Die Nutzung des Redaktionswerkzeuges durch die Verwaltungen darf jedoch keine Sicherheitsprobleme im Berliner Verwaltungsnetz hervorrufen. Bei einer Nutzung über das Internet ist – wenn möglich – der zentrale Übergang des Landesbetriebs für Informationstechnik[67] zu verwenden. Für jede andere Nutzungsart, z. B. über einen Internet-Provider oder über die Modem-Einwahl, dürfen die Rechner, von denen die Nutzung des Redaktionswerkzeuges aus erfolgt, aus Datenschutz- und IT-Sicherheitgründen nicht an das lokale Netz der jeweiligen Verwaltung und damit an das MAN angeschlossen sein. Jeder weitere Anschluss an externe Netze, der nicht durch dem hohen Schutzbedarf des MAN entsprechende Sicherheitsmechanismen abgesichert wird, stellt eine Umgehung des Firewall-Systems des MAN dar und birgt erhebliche sicherheitstechnische Gefahren für alle an das MAN angeschlossenen Systeme.

Exemplarische IT-Projekte der Berliner Verwaltung

Das Berliner Datenschutzgesetz sieht in § 24 Abs. 3 Satz 3 vor, dass der Berliner Datenschutzbeauftragte über die Einführung neuer Informationsvorhaben im Bereich der Behörden und sonstigen öffentlichen Stellen zu informieren ist. Diese *Informationspflicht* ist ein sehr wichtiges Instrument, um dem Datenschutz bei der Einführung neuer Verfahren Gewicht zu verleihen. Sie gibt uns die Möglichkeit, die Planungsunterlagen auf datenschutzrechtliche Aspekte zu überprüfen und bei Bedarf mit unserer Stellungnahme Einfluss zu nehmen, bevor die Projekte eine Reife erlangen, in denen Modifikationen nur noch mit Aufwand möglich sind. Voraussetzung dafür, dass wir uns beratend an der Durchführung der Projekte beteiligen, ist, dass die Unterrichtung so rechtzeitig erfolgt, dass auch unter Berücksichtigung einer gewissen Zeit zur Bearbeitung der gelegentlich mehrere Ordner umfassenden Unterlagen aus rechtlicher und aus technisch-organisatorischer Sicht noch eine Beeinflussung des Projektes möglich ist. Andererseits wollen wir nur zu Materialien Stellung nehmen, die einen hinreichenden Bearbeitungsstand erreicht haben, so dass wir davon ausgehen können, dass unsere Stellungnahme nach Fertigstellung nicht schon gegenstandslos ist.

Die *Unterrichtungspflicht* wird von den öffentlichen Stellen in sehr unterschiedlicher Weise wahrgenommen. Einige Stellen informieren offensiv, ausführlich und frühzeitig, andere ausgesprochen zurückhaltend, knapp und verspätet, manche unterrichten überhaupt nicht, wohl in der Annahme, die Intervention des Datenschutzbeauftragten würde zu Projektverzögerungen führen. Es gibt auch Stellen, die offenbar grundsätzlich von der Vorstellung geleitet werden, dass es primäre Pflicht des Datenschutzbeauftragten sei, IT-Projekte zu verhindern. Das Gegenteil ist der Fall: Primäre Pflicht des Datenschutzbeauftragten ist es, IT-Projekte konstruktiv zu begleiten, damit sie auch in datenschutzrechtlicher Hinsicht und im Hinblick auf die informationstechnische Sicherheit optimal gestaltet sind. Insoweit sehen wir uns als Teil der Qualitätskontrolle.

Das Projekt *„Integrierte Personalverwaltung – IPV",* welches auf der Basis von SAP R/3[68] entwickelt wird, erlebte einen Einschnitt, als die Firma KPMG, die bis dahin mit dem „Customizing" beauftragt war, die Zusammenarbeit mit der Projektgruppe beendete. Die Firma SAP übernahm daraufhin selbst die Kundenanpassung, wobei deutlich gemacht wurde, dass die bisherigen Projektvoraussetzungen zu überprüfen seien. Wir sahen darin auch Risiken für die im Rahmen unserer Einbindung erzielten Ergebnisse. Wir gehen aufgrund der daraufhin geführten Gespräche davon aus, dass unsere Sorge unbegründet war und dass unsere bisherigen Hinweise weiterhin Beachtung finden. Ein Thema war der beabsichtigte Fernzugriff der Firma SAP zur Beseitigung von Störungen. Dieser erfolgt so beschränkt und kontrollierbar, dass wir unsere Bedenken zurückstellen konnten. Häufiger Diskussionspunkt war die Verschlüsselung der Datenübertragung auf dem Berliner Landesnetz. Zwar ist unstrittig, dass sie bei der Übertragung der Personaldaten der Mitarbeiter des Landes erfolgen muss, jedoch blieb lange

67 Grenznetz: JB 1997, 2.3

68 siehe 4.8

unklar, ob die verfahrensunabhängige Verschlüsselung auf dem Netz, die der LIT anbietet, für das Projekt nutzbar gemacht werden kann. Ergebnisse liegen noch nicht vor.

Das *„Berliner Automatisierte Sozialhilfe-Interaktions-System – BASIS“* in den Bezirksämtern und in der Zentralen Leistungsstelle für Asylbewerber ist in vollem Umfang in Betrieb. Gleichzeitig wird das Nachfolgeprojekt BASIS II bzw. BASIS 3000 weiter vorangetrieben. Mit dem „Technischen Piloten“ wurde eine erste Komponente des neuen Verfahrens in Betrieb genommen, die dem überbezirklichen Abgleich zur Erkennung des Sozialhilfemissbrauchs dienen soll.

Die Einführung einer *elektronischen Geldbörse* zur Gewährung von Sachleistungen für Asylbewerber hat großes öffentliches Aufsehen erregt[69].

Im Landesamt für Gesundheit und Soziales wird ein *„Online-Schwerbehinderten-Anwendungs-Verfahren – OSAV“* entwickelt.

Der Bereich der *Justiz* wurde in der Vergangenheit immer wieder öffentlich als rückständig hinsichtlich der Anwendung moderner Informationstechnologien dargestellt. Dem widersprechen starke Aktivitäten bei der Durchführung von IT-Projekten.

Die Projekte *AULAK (Automatisches Verfahren Land-, Amts- und Kammergericht), KOKA (Geschäftsstellenautomation in Konkurssachen), JUKOS (Justiz-Kostenbearbeitung – Vollstreckung von Geldstrafen)* sind Beispiele für eine Reihe von Projekten, die insbesondere im Bereich der *Gerichte* zur Arbeitsbeschleunigung führen sollen.

Die Projekte *BIDAVIS zur Bilddatenverarbeitung* und *FABIS zur Fingerabdruckverarbeitung* erleichterten die Arbeit des Erkennungsdienstes der Polizei.

Das Gleiche gilt für das *ADV-Verfahren BOWI II zur Bearbeitung von Verkehrsordnungswidrigkeiten.* Hier soll ein externes Unternehmen die Erstellung und den Betrieb des Verfahrens übernehmen. Dieses ist datenschutzrechtlich unbedenklich, soweit damit keine Übertragung hoheitlicher Aufgaben verbunden ist und der Datenverkehr zwischen dem Dienstleister und der Bußgeldbehörde unter Berücksichtigung der notwendigen Sicherheitsmaßnahmen zur Gewährleistung der Vertraulichkeit der Daten bei der Übertragung (Verschlüsselung) und zum Schutz der angeschlossenen Systeme (Firewalls) erfolgt. Weitere Fragestellungen ergaben sich aus der elektronischen Archivierung der abgeschlossenen Verfahren, weil diese aus Rationalisierungsgründen so organisiert wird, dass Restrisiken für die Integrität der archivierten Informationen bleiben. Diese werden als hinnehmbar eingeschätzt.

[69] vgl. 4.4.3

3. Schwerpunkte im Berichtsjahr

3.1 Wer nicht löschen will, muss büßen

Eine intensive öffentliche Diskussion löste der Vollzug einer Vorschrift des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) aus, die den Polizeipräsidenten verpflichtet, alle Betroffenen, deren Daten länger als fünf Jahre im *Informationssystem Verbrechensbekämpfung* (ISVB) gespeichert sind, hierüber zu informieren (§ 43 Abs. 3). Der Gesetzgeber hatte diese Vorschrift 1992 in das ASOG in der Erwartung aufgenommen, dass diese Verpflichtung zu einer besonderen Zurückhaltung bei der längerfristigen Speicherung von Daten führen würde. Der Polizeipräsident hat diese Erwartung nicht erfüllt.

So stellte man fünf Jahre nach In-Kraft-Treten des neuen ASOG (also nicht nach Einspeicherung der Daten, mit der eigentlich die Fristen zu laufen beginnen) fest, dass über 750 000 Personen *unterrichtet* werden mussten – und nicht etwa nur Tatverdächtige, bei denen wegen der Schwere des Tatvorwurfs eine so lange Speicherung zur vorbeugenden Straftatenbekämpfung erforderlich sein mag. Vielmehr befanden sich darunter in der Mehrzahl Verdächtige weniger schwerer Straftaten und Anzeigeerstatter. Entsprechend empört reagierten die Adressaten der ersten 80 000 Briefe, die die Polizei im Juli 1998 verschickte. Dies auch, weil die Betroffenen zunächst im Unklaren darüber gelassen wurden, ob sie als Tatverdächtige oder Anzeigeerstatter registriert sind. Nicht minder empört waren Öffentlichkeit und Politiker wegen der damit verbundenen Kosten. Leider richtete sich der Zorn häufig gegen die Mitteilungspflicht, nicht aber gegen die Praxis der Polizei, die der Intention des Gesetzgebers zuwider lief und die durch die Missachtung oder zumindest bürgerunfreundliche Interpretation des ASOG überhaupt erst entstanden war.

Wir wurden bei der Vorbereitung der Benachrichtigungsaktion nicht beteiligt. Die später von uns durchgeführte Überprüfung führte zu Ergebnissen, die in mehrfacher Hinsicht eine Änderung der Vorgehensweise der Polizei erforderlich machen.

Lösch- und Prüffristen

Wer erwartet hätte, dass das ASOG angesichts der Sensitivität der Daten besonders klar zum Ausdruck bringt, innerhalb welcher Fristen welche Daten zu löschen sind, wird enttäuscht: Entgegen unserem Votum im Gesetzgebungsverfahren zur Neufassung des ASOG sind dort klare *Löschungsfristen* nur für die Daten von Kontaktpersonen von Verdächtigen, Zeugen, Hinweisgebern und Auskunftspersonen vorgesehen, mithin Personen, die selbst nicht verdächtigt worden sind und gleichwohl eine Speicherung zur vorbeugenden Straftatenbekämpfung dulden müssen – nämlich drei Jahre. Für die Verdächtigen selbst, egal ob sich der Verdacht bestätigt hat oder nicht, wurden nur Prüffristen festgelegt und zwar nicht im Gesetz selbst, sondern in einer eigenen

„Verordnung über Prüffristen bei polizeilicher Datenspeicherung“ *(Prüffristenverordnung)*. Überhaupt keine Fristen gibt das ASOG vor, wenn die Daten nicht zur vorbeugenden Straftatenbekämpfung gespeichert werden, sondern zur Vorgangsverwaltung oder zur Dokumentation – die „zeitlich befristet“ sein soll, ohne dass gesagt wird, was das heißt (§ 42 Abs. 1 ASOG).

Diese unklaren Vorgaben sind für einen Teil der Probleme verantwortlich.

So legte der Polizeipräsident als Frist für die Speicherung zu *Vorgangsverwaltung und Dokumentation* pauschal fünf Jahre fest, mit der Folge, dass Daten von Anzeigeerstattern genauso lange im System blieben wie diejenigen von Straftätern und zwei Jahre länger als Daten z. B. von Personen, die enge Kontakte zu Straftätern hatten. Jahrelange Forderungen von uns, die Fristen zu verkürzen, hatten keinen Erfolg.

Auch bei der Anwendung der Prüffristenverordnung wird nicht etwa so vorgegangen, dass zugunsten der Betroffenen Prüffristen (die eine Prüfung, nicht etwa schon eine Löschung vorschreiben) möglichst kurz gehalten werden. Vielmehr wird regelmäßig die Höchstfrist von zehn Jahren festgelegt, die verringerte Frist von fünf Jahren bei Fällen von geringer Bedeutung wird äußerst restriktiv gehandhabt, so wird bereits bei einem Schaden von mehr als 100 DM davon ausgegangen, dass es sich um einen schwerwiegenden Fall handelt, der eine Prüfung erst nach 10 Jahren erforderlich macht. Nur bei Jugendlichen und über 70-Jährigen verkürzt die Verordnung selbst auf die Höchstfrist von fünf Jahren. Von den vom Verordnungsgeber vorgesehenen zusätzlichen Verkürzungsmöglichkeiten (das bedeutet bei Erwachsenen Fristen von einem Jahr bis fünf Jahren, nicht mindestens fünf Jahre) wird fast gar kein Gebrauch gemacht.

All dies führte dazu, dass in einer weitaus überwiegenden Zahl der Fälle personenbezogene Daten im ISVB mindestens fünf Jahre gespeichert blieben, bevor sie überprüft (Verdächtige) oder gelöscht wurden. Zu berücksichtigen ist dabei, dass die Prüfung natürlich nicht am Tage des Fristablaufs erfolgen kann, sondern dass es hierbei auch Vorlauf- und Bearbeitungszeiten gibt (nicht unter zwei Monaten). Da aber die Mitteilungspflicht bereits mit fünf Jahren eintritt, erfasst sie nach der bestehenden Praxis auch die Daten, die – eventuell nach Prüfung – nach dieser Frist schon hätten gelöscht werden müssen.

Eine wichtige Konsequenz ergibt sich schon aus diesem systematischen Mangel: Löschungsfristen müssen so festgelegt werden, dass die Daten vor Eintritt der Benachrichtigungspflicht gelöscht sind, Prüffristen bei nicht schwerwiegenden Fällen müssen so eingerichtet werden, dass die Prüfung einschließlich der dabei verfügten Löschung vor Ablauf von fünf Jahren abgeschlossen ist.

Die Fristenspirale

Noch gravierender als die Folgen der Fristfestlegung selbst sind die Folgen der Praxis in den Fällen, in denen zu vorhandenen Daten neue Daten hinzukommen. Gleich, ob es sich um Daten von Verdächtigen oder anderen Personen wie Anzeigeerstattern handelt, lässt die Speicherung neuer Daten die Fristen erneut von vorne beginnen: Wem viereinhalb Jahre nach Anzeige eines Fahrraddiebstahls nunmehr die Geldbörse aus der Tasche gezogen wurde, muss damit rechnen, dass der Fahrraddiebstahl fast zehn Jahre, oder – wenn er nach Jahren erneut Opfer von Strafen wird – beliebig lange im System registriert bleibt. Dies führt sinnloserweise wegen der Verlängerung der Speicherungsdauer wiederum zur Benachrichtigungspflicht. Ein großer Teil der Benachrichtigungen kann allein durch die Abschaffung dieser „Fristenspirale“ bei Anzeigeerstattern entfallen.

Die für Tatverdächtige zur Erkennung von Wiederholungstätern ersonnene Fristenspirale ist bei der Speicherung von Daten in bestimmten Fällen nicht verhältnismäßig. Wer vor vier Jahren wegen einer Beleidigung registriert wurde, muss nicht hinnehmen, dass diese Datenspeicherung beispielsweise wegen eines Ladendiebstahls um weitere fünf Jahre verlängert wird. Dies hat im Übrigen auch der Bayerische Verwaltungsgerichtshof festgestellt[70].

Überwachung der Prüffristen

Diese unbefriedigenden Vorgaben dürfen nicht zu dem Eindruck führen, dass die Polizei keine Mühe auf die Prüfung der Notwendigkeit von Datenspeicherungen verwendet. Vielmehr ist ein aufwendiges *Verfahren zur Überwachung der Speicherung* entwickelt worden.

Die Überwachung der Prüffristen erfolgt monatlich in vier Phasen:

Am zweiten Tag eines Monats werden bis auf wenige Ausnahmen die Personalien aller Personen, die länger als zwei Jahre verstorben sind und zu denen eine Sterbemitteilung vorliegt, automatisch aus allen Bezugsvorgängen herausgelöst und gelöscht. Über diese Löschung wird eine Druckliste als Protokoll erstellt. Sie enthält Hinweise auf vorhandene Akten. Diese Liste wird der Aktenhaltung und – sofern erkennungsdienstliches Material vorhanden ist – der hierfür zuständigen Stelle übersandt.

Danach werden alle Vorgänge, die länger als zehn Jahre gespeichert sind, hinsichtlich des aktuellen Personen-, Sach- oder Kfz-Fahndungsbestandes überprüft. Der Vorgang wird im ISVB automatisch gelöscht, wenn kein Fahndungsbestand vorhanden ist.

---

70 Beschluss vom 4. Juni 1996, Az.: 94, 3094

Nunmehr werden die Prüffristen der Tatverdächtigen überprüft. Die Aktenhaltung stellt anhand des Vorganges fest, ob seit dem Zeitpunkt des Festlegens der letzten Prüffrist Angaben zur Person des Betroffenen (Speicherung im ISVB und/oder neue Unterlagen in der Kriminalakte) ergänzt worden sind. Ist dies nicht der Fall, werden die Daten im ISVB gelöscht und die dazugehörigen erkennungsdienstlichen Unterlagen vernichtet. Sofern allerdings während der laufenden Prüffrist weitere Unterlagen bzw. Speicherungen hinzugekommen sind, wird die Frist verlängert sowie im ISVB gespeichert.

In keinem der von uns überprüften Einzelfälle waren die Entscheidungsgründe für eine Festlegung bzw. Verlängerung der Prüffrist in der Akte dokumentiert. Auch inwieweit die Erforderlichkeit des Verbleibes von Altdaten zum Zweck der vorbeugenden Straftatenbekämpfung überprüft wurde, lässt sich anhand des Akteninhaltes nicht verifizieren. Als Beleg für die Durchführung der Überprüfung der Speicherfristen wird der Akte lediglich ein Blatt, auf dem der nächste Prüftermin festgehalten ist, beigefügt. Die Verlängerung der Prüffristen erfolgt schematisch nach den Vorgaben eines internen „Arbeitsbogens“. Entweder wird erneut die Höchst- oder die verkürzte Prüffrist vergeben. Eine – auch für den Außenstehenden – nachvollziehbare Revision des behördlichen Handelns bzw. der getroffenen Entscheidung ist so nicht möglich. Verschiedentlich wurde die Verlängerung der Prüffrist lediglich auf den ISVB-Auszug aus der Monatsliste gestützt, ohne dass Unterlagen zu dem Vorgang vorhanden waren.

Im letzten Arbeitsschritt werden die Personendatensätze von Anzeigenden und Geschädigten gelöscht, wenn das letzte Bearbeitungsdatum länger als fünf Jahre zurückliegt und kein Fahndungsbestand vorliegt.

Die Benachrichtigung der Betroffenen

Die Unterrichtung der Personen, deren Daten länger als fünf Jahre im ISVB gespeichert sind, erfolgte in wenig bürgerfreundlicher Weise. Mit Erschrecken lasen viele Bürger den Brief der Polizei, in dem ihnen mitgeteilt wurde, dass ihre Daten im Informationssystem Verbrechensbekämpfung gespeichert sind, aber aus technischen Gründen im Zuge dieser automatisierten Benachrichtigung leider nicht unterschieden werden könne, ob eine Speicherung als Tatverdächtiger oder Anzeigender oder Geschädigter vorgenommen wurde. Kein Wunder, dass die Telefone bei uns und der Polizei daraufhin nicht mehr stillstanden. Die Polizei änderte das Unterrichtungsschreiben bald darauf und klärte in der nächsten Aktion die Betroffenen darüber auf, ob sie als Tatverdächtige oder Anzeigenerstatter registriert sind. Die Beschwerden der Bürger haben seitdem abgenommen. In vielen Fällen führte die Unterrichtung aber nach Auskunftsanträgen der Betroffenen zu Datenlöschungen oder Berichtigungen.

Im Januar 1999 hat die Polizei die Speicherungsdauer für Daten von Anzeigenerstattern im ISVB auf drei Jahre verkürzt. Eine Entscheidung der Polizei über verkürzte Prüffristen auch bei Tatverdächtigen steht noch aus.

3.2 Trautes Heim – Job on-line

Bei der Diskussion um rationelle Formen der Arbeitsorganisation spielt der Begriff der *„Telearbeit“* eine zunehmende Rolle. Vordergründig handelt sich dabei um eine neue Organisationsform, die erst durch die Informations- und Kommunikationstechnik möglich geworden ist. Sie erlaubt es, Arbeiten, die zuvor nur in Büroräumen der Dienststelle oder des Unternehmens möglich waren, an anderen Orten zu erbringen. Die Arbeitsaufträge werden on-line abgewickelt, das leidige Pendeln vom Wohnort zur Arbeitsstelle und zurück wird reduziert. Vorteilhaft für den Beschäftigten ist die Autonomie bei der Zeiteinteilung, die mit Vorteilen der Flexibilisierung von Arbeitszeit und -platz (einschließlich der Einsparung von Büroräumen) für den Arbeitgeber verbunden ist.

Die seit Jahrzehnten in vielen Forschungsprojekten und Publikationen theoretisch erörterten Ausgestaltungsmöglichkeiten werden mit zunehmender Geschwindigkeit realisiert. Während lange in der Forschungslandschaft der Spruch umging, es gebe mehr Forscher, die sich mit der Telearbeit beschäftigten, als Menschen, die Telearbeit verrichteten, eroberte die Telearbeit in den vergangenen Jahren mehr und mehr Terrain.

Auf globaler Ebene ist die fern vom Unternehmen stattfindende Softwareproduktion in Ländern mit hohem Ausbildungsstandard und gleichwohl günstigen Lohnkosten (wie Indien oder die baltischen Staaten), die weltweite Zusammenarbeit spezialisierter Firmen bei der Entwicklung moderner Technologie durch gemeinsame Produktentwicklung mit Hilfe moderner Designtechnologie oder die Ausnutzung der weltweiten Zeitzonen für das Angebot von Call-center-Diensten, die rund um die Uhr arbeiten, ohne dass Nachtschichten erforderlich wären, in aller Munde. Soweit personenbezogene Daten verarbeitet werden, sind zur Sicherstellung des Datenschutzes hier weltweite Abkommen erforderlich – das Problem ist erkannt, wenn auch noch eine Lösung nicht in Sicht ist.

Die globale Dimension des Problems überdeckt allerdings allzu leicht, dass sich die Tendenz, durch Arbeitsleistungen außerhalb der Dienststelle zu einer Rationalisierung des Arbeitsablaufs zu kommen, auch in kleinerem Rahmen Bahn bricht. Auch *im lokalen Rahmen* wird das Bedürfnis stärker, Arbeit entfernt vom Büroplatz zu verrichten, sei es um kostengünstige Filialen zu errichten, auf Dienstreisen und bei anderen längeren Abwesenheiten gleichwohl arbeiten zu können oder trotz Kinderbetreuung oder anderer familiärer Umstände zumindest eine Teilzeitbeschäftigung wahrnehmen zu können.

Die Akzeptanz ist groß: 1998 haben sich nach Abschluss eines dreijährigen Pilotprojekts die Deutsche Telekom AG und die Deutsche Postgewerkschaft auf einen *Tarifvertrag über Telearbeit* geeinigt. Von den Teilnehmern des Pilotprojekts hatten sich 97,8 % für eine Fortführung der Telearbeit ausgesprochen.

Auffallend, aber gleichwohl nicht überraschend ist bei alldem die überwiegende Behandlung sozialer Aspekte der Telearbeit, weniger jedoch die Beschäftigung mit datenschutzrechtlichen Problemen. Hier stellen sich jedoch Probleme, die gelöst werden müssen, damit die Telearbeit auch unter Aspekten des Datenschutzes akzeptabel ist. Diese Probleme sind nicht neu, sie haben sich schon immer ergeben, wenn Unterlagen aus dem Verfügungsbereich des Unternehmens oder der Behörde zur Bearbeitung herausgegeben oder -genommen wurden. Neu ist das Hinzukommen der Informations- und Kommunikationstechnik, sei es in der Form der isolierten Nutzung eines häuslichen PC oder gar der Vernetzung.

Am häufigsten war das der Fall, wenn Arbeiten zu Hause erledigt werden sollten: Die traditionelle *Heimarbeit* ist Ausgangspunkt der modernen Telearbeit. Der Regelfall ist, dass gestattet wird, einen Teil der Arbeitszeit zu Hause zu verrichten (alternierende [Tele-]Heimarbeit). Für bestimmte Berufe sowohl im öffentlichen (Lehrer, Richter) als auch im privaten Bereich (Außendienstmitarbeiter) gehört es zum Berufsbild, dass ein mehr oder weniger großer Teil der Arbeit, für die der Umgang mit personenbezogenen Daten wesentlich ist, zu Hause verrichtet wird. Daneben gab es schon immer Betätigungen, die von vornherein ausschließlich zu Hause verrichtet wurden (Gerichtsvollzieher, selbständige Handelsvertreter), obwohl sie in einen dienstlichen Zusammenhang eingebettet waren.

Hinzu treten neue Organisationsformen wie Satellitenbüros (Zweigstellen eines Unternehmens in Wohnraumnähe) oder Nachbarschaftsbüros (Arbeitsmöglichkeit für verschiedene Unternehmen).

Voraussetzungen

Unabhängig davon, ob Telearbeit in der öffentlichen Verwaltung oder in einem Privatunternehmen geleistet werden soll, kommen grundsätzlich zwei Vertragsformen in Betracht: Sie kann im Rahmen eines Dienst- oder Arbeitsverhältnisses vereinbart werden, das ganz oder teilweise aus der Ferne abgewickelt wird, oder sie ist Bestandteil eines Werkvertrags.

Aus datenschutzrechtlicher Sicht liegt der Unterschied in dem verschiedenen Verantwortungsumfang für die personenbezogenen Daten, die verarbeitet werden sollen. Bei einer *arbeits- oder dienstrechtlichen Vereinbarung* bleibt der Telearbeiter Teil der Dienststelle bzw. des Unternehmens, sein Zugriff auf die Daten stellt eine Nutzung dar, deren Zulässigkeit sich allein nach den materiellen, für den Arbeitgeber geltenden Bestimmungen richtet. So sind Lehrer und Richter in der gleichen Weise zum Umgang mit den Daten verpflichtet, wie dies in der Dienststelle der Fall wäre, Arbeitnehmer, die zu Hause arbeiten, in der gleichen Weise befugt wie im Betrieb.

Gestattet der Arbeitgeber Heimarbeit in einem bestimmten Umfang oder wird von vornherein Heimarbeit arbeitsvertraglich oder dienstrechtlich vereinbart, sind allerdings in die Vereinbarungen *Datenschutzklauseln* aufzunehmen, die den Umfang der zulässigen Verarbeitung personenbezogener Daten regeln. Sie müssen zwar nicht die Befugnis zur Verarbeitung der Daten selbst umfassen, da sich diese ja bereits aus dem Arbeits- bzw. Dienstverhältnis ergibt. Je nach der Arbeitssituation zu Hause muss aber bestimmt werden, welche Daten mitgenommen werden dürfen bzw. auf welche Daten online zugegriffen werden darf sowie welche Sicherungsvorkehrungen zu treffen sind.

Anders sieht es aus, wenn die Telearbeit verselbständigt wird. Wird die Verarbeitung von Daten, etwa zu Erstellung von Schriftstücken, *im Rahmen eines Werkvertrages* vereinbart, handelt es sich um Datenverarbeitung im Auftrag, bei der die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeitet werden dürfen. Diese müssen vertraglich festgelegt werden. Noch weiter würde eine Funktionsübertragung gehen[71], bei der der (selbständige) Telearbeiter über den Umfang der Verarbeitung der Daten selbst entscheiden kann. Die Verträge müssen hier sicherstellen, dass sich die Verwertung der Daten des Auftraggebers im Rahmen der Zweckbestimmung der Übermittlung hält.

Welche Form auch immer gewählt wird: Die Verantwortlichkeit der Stelle, in deren Bereich die personenbezogenen Daten verarbeitet werden, muss durch organisatorische Vorkehrungen abgesichert werden. Hierzu gehört, dass festgelegt wird, wer über den Umfang der Telearbeit in welcher Form auch immer zu entscheiden hat und wer im konkreten Einzelfall die Herausgabe personenbezogener Daten verantwortet.

Sparsamkeitsprinzip

Die Herausgabe personenbezogener Daten aus dem räumlichen Bereich der Dienststelle birgt immer *Risiken:* Bei herkömmlichen Unterlagen ist dies der Verlust durch mangelnde Aufmerksamkeit – Aktenfunde auf der Straße oder in der U-Bahn sind nach wie vor in der Presse beliebte Skandale –, aber auch die Möglichkeit der Einsichtnahme durch Familienangehörige oder andere Personen in der Wohnung. Bei der Nutzung der IuK-Technik kommen die Möglichkeiten der Einsichtnahme und – hier verstärkt – der Fälschung durch Personen in Betracht, die Zugang zu der Datenverarbeitung haben, sei es auf dem Übermittlungsweg, sei es am Telearbeitsplatz.

[71] JB 1997, 4.8.1

Daraus folgt vor allem, dass die Verarbeitung personenbezogener Daten im Rahmen von Telearbeit auf das erforderliche Minimum beschränkt werden, ja dass die Verarbeitung bestimmter Datenarten, etwa *medizinischer Daten,* grundsätzlich ausgeschlossen werden muss. Dies macht Heim- und Telearbeit nicht unmöglich: Vielmehr ist nach Wegen zu suchen, ohne Personenbezug auszukommen.

Eine Möglichkeit ist, die Telearbeit auf Bereiche zu beschränken, bei denen personenbezogene Daten nicht vorkommen. Dies wird allerdings häufig kein gangbarer Weg sein. Als nächste Möglichkeit bietet sich die *Pseudonymisierung* an: Die identifizierenden Daten (insbesondere Name, Geburtsdatum und Adresse) werden durch Merkmale (z. B. Ziffern) ersetzt, mit deren Hilfe nur der Arbeitgeber selbst, aber nicht der Telearbeiter auf die Betroffenen rückschließen kann.

Ein Krankenhaus bat um Auskunft, ob es statthaft sei, wegen der bestehenden Raumnot Schreibarbeiten an fest angestellte Mitarbeiterinnen des Klinikums in Heimarbeit zu vergeben.

Grundsätzlich dürfen personenbezogene Daten, die einem Berufs- und besonderen Amtsgeheimnis unterliegen, nicht in Heimarbeit verarbeitet werden. Um derartige hochsensible Daten handelt es sich jedoch in den von den Schreibkräften anzufertigenden Arztberichten. Dies ist jedoch nicht mehr der Fall, wenn die Unterlagen, die im Rahmen der Heimarbeit anfallen, nicht (mehr) personenbezogen sind. In diesem Fall wäre Heimarbeit möglich.

Denkbar ist z. B., dass die Ärzte ihre Berichte von vornherein in pseudonymer Form, also unter Ausschluss identifizierender Daten abfassen. Die einzelnen Berichte erhielten dabei in der Entwurfsphase lediglich spezielle Kennzahlen, die dem jeweiligen Patienten zugeordnet sind (evtl. die Patientennummer). Nach Fertigstellung der Berichte könnten diese dann in den Diensträumen um die Personalien des Patienten ergänzt werden.

Technisch-organisatorische Maßnahmen

Ist es nicht möglich, die Heimarbeit auf die Verarbeitung anonymer Unterlagen zu beschränken, sind besondere technische und organisatorische Maßnahmen zu ergreifen, um den Schutz der personenbezogenen Daten zu gewährleisten.

Werden im Rahmen der Heimarbeit Unterlagen transportiert, seien es Akten, Diktierbänder oder Datenträger, müssen *Vorkehrungen gegen die unbefugte Wegnahme oder Kenntnisnahme Dritter* getroffen werden. So sollte in den Telearbeitsvertrag die Verpflichtung des Telearbeiters aufgenommen werden, das Fahrzeug oder die Aktentasche mit den Unterlagen nicht unbeaufsichtigt stehen zu lassen.

Sichergestellt werden muss auch, dass die Unterlagen und Datenträger so untergebracht werden können, dass eine unbefugte Nutzung ausgeschlossen wird (abschließbarer Schreibtisch, Schrank etc.). Die *Beschaffung bzw. Bereitstellung der erforderlichen IT-Ausstattung* (Geräte, Betriebssysteme, verwendete Standard- und Anwenderprogramme, Einrichtungen zur Datenfernverarbeitung) ist grundsätzlich Aufgabe des Arbeitgebers, der damit die Art und Weise der Verarbeitung der Daten bestimmen kann. Änderungen und Ergänzungen dürfen dann natürlich nur mit ausdrücklicher Zustimmung des Arbeitgebers erfolgen.

Erfolgt die Heimarbeit in Form eines *Werkvertrags,* wird der Heimarbeiter die Arbeitsmittel in der Regel selbst beschaffen. Hier müssen klare Vorgaben gegeben werden, die eine vertragswidrige Nutzung der Daten mit Hilfe der verwendeten Technik ausschließen. So muss sichergestellt werden, dass die im Rahmen des Werkvertrags verarbeiteten Daten nicht auf Geräten vorgehalten werden, in die z. B. wegen eines auf dem Gerät realisierten Zugangs zum Internet von außen eingedrungen werden kann – die bei größeren Teleanwendungen selbstverständlich einzurichtenden Firewalls[72] dürften im Normalfall der Teleheimarbeit zu aufwendig sein.

Bei der Nutzung der IuK-Technik sind alle datenschutzrechtlichen Anforderungen an Technik und Organisation umzusetzen. Besondere Bedeutung für die Sicherung der Integrität und Vertraulichkeit hat die *Zugriffskontrolle.* Bei der Heimarbeit kommt der Absicherung des Telearbeitsplatzes gegen die unbefugte Nutzung Dritter (Familienangehöriger, Nachbarn, Freunde etc.) besondere Bedeutung zu. Die *Verschlüsselung* der auf dem Telearbeitsplatz gespeicherten personenbezogenen Daten ist neben gängigen Authentifizierungsverfahren (Pin-Code, Chipkarte u. Ä.) das geeignetste Instrument gegen Missbrauch.

Unter den „zehn Geboten“ zur Datensicherung befindet sich auch die Verpflichtung zur *Eingabekontrolle,* d. h. es muss möglich sein, nachträglich festzustellen, welche personenbezogenen Daten zu welcher Zeit von wem in das Datenverarbeitungssystem eingegeben wurden. Es sind daher Maßnahmen zu treffen, um die Authentizität des Telearbeiters, etwa mit Hilfe der *digitalen Signatur,* zu gewährleisten.

Schutz der Privatsphäre des Teleheimarbeiters

Mit jeder Form der Heimarbeit ist ein Eindringen in die Privatsphäre verbunden. Da keine unmittelbare Arbeitszeitkontrolle möglich ist, muss Heimarbeit jedenfalls dann in besonderer Weise protokolliert werden, wenn sie im Rahmen eines Arbeitsvertrags oder Dienstverhältnisses erfolgt – nur bei einer werkvertraglichen Lösung ist eine solche Kon-

[72] vgl. 2.2

trolle nicht erforderlich. Nahe liegt, die aus datenschutzrechtlichen Gründen erforderliche *Protokollierung* auch zur Arbeitszeiterfassung zu nutzen. Dem steht allerdings die Zweckbindung der für die Datensicherung erhobenen Daten entgegen; diese dürfen für keine anderen Zwecke, mithin auch nicht zur Leistungs- und Verhaltenskontrolle genutzt werden (§§ 14 Abs. 4, 31 BDSG, 11 Abs. 5 BlnDSG). Für die Heimarbeitsvereinbarung ist ein Weg zu finden, der eine Protokollierung der Arbeitszeit unter möglichst hoher Wahrung der Privatsphäre ermöglicht. Dies ist gerade in den Fällen bedeutsam, in denen Heimarbeit wegen der familiären Verhältnisse vereinbart wird – es wäre inakzeptabel, wenn aus den Telearbeitsprotokollen die Stillzeiten junger Mütter ableitbar wären.

Gravierender ist ein anderes Problem: Die Kontrollierbarkeit der Datenverarbeitung ist ein wesentlicher Grundsatz des Datenschutzes. Sie muss auf zwei Ebenen gewährleistet sein: Zum einen gegenüber dem Arbeitgeber und Dienstherrn, die diese Kontrolle in der Regel durch die betrieblichen bzw. behördlichen Datenschutzbeauftragten ausüben, zum anderen gegenüber den *externen Kontrollinstanzen,* der Aufsichtsbehörde bzw. dem Datenschutzbeauftragten (die in Berlin in einer Hand liegen). Wird Heimarbeit geleistet, setzt die Kontrollierbarkeit den Zugang der Kontrollstellen zum Arbeitsplatz in der Privatwohnung voraus.

Für betriebliche und behördliche Datenschutzbeauftragte sehen die Datenschutzgesetze hierfür keine besonderen Befugnisse vor. Damit haben diese keine gesetzliche Möglichkeit zum *Betreten der Privatwohnung,* die ja in besonderem Maße grundrechtlich geschützt ist (Art. 13 GG). Da aber das Unternehmen oder die Behörde für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist (§§ 18, 36 BDSG, 19 Abs. 1 BlnDSG), muss auch hier die Kontrolle gewährleistet bleiben. Dies bedeutet, dass in die Vereinbarungen über die Heimarbeit entsprechende *Zutrittrechte* aufzunehmen sind, die allerdings dem Grundrechtsgehalt des Art. 13 GG Rechnung zu tragen haben. Entsprechendes muss auch gelten, wenn die Telearbeit im Wege der Auftragsdatenverarbeitung vereinbart wurde.

Für Aufsichtsbehörden und Datenschutzbeauftragte ist die Situation scheinbar einfacher: Die Aufsichtsbehörden können bei Privatunternehmen, soweit dies für Prüfungen erforderlich ist, „während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume“ betreten und „dort Prüfungen und Besichtigungen“ vornehmen (§ 38 Abs. 4 BDSG). Dem Berliner Datenschutzbeauftragten ist von öffentlichen Stellen des Landes „jederzeit Zutritt in alle Diensträume“ zu gewähren (§ 28 Abs. 1 S. 1 Ziff. 3 BlnDSG). Diese Befugnisse gelten in den Fällen unbeschränkt, in denen die Telearbeitsplätze als Geschäfts- oder Diensträume betrachtet werden können. Dies ist allerdings nur dann der Fall, in denen Daten auf werkvertraglicher Basis im Auftrag verarbeitet werden oder der häusliche Arbeitsplatz als Dienstraum gewertet wird (wie dies z. B. bei Gerichtsvollziehern der Fall ist).

In allen anderen Fällen gebietet das *Grundrecht auf Unverletzlichkeit der Wohnung,* dass eine ausdrückliche Einwilligung in das Betretungsrecht des Datenschutzbeauftragten abgegeben wird. Sie ist die Voraussetzung für eine rechtmäßige Vereinbarung von Heimarbeit.

Internationale Aspekte

Telearbeit hat in den letzten Jahren im Rahmen der europäischen Wirtschaftspolitik Aufmerksamkeit gewonnen. An zentraler Stelle des den europäischen Binnenmarkt prägenden *Weißbuchs für Wachstum, Wettbewerbsfähigkeit und Beschäftigung*[73] finden sich bereits Hinweise des ehemaligen Präsidenten der Europäischen Kommission, Jaques Delors, auf die Möglichkeiten der Telearbeit. Inzwischen ist anerkannt, dass nationale gesetzliche Rahmenbedingungen für die Telearbeit nicht ausreichend sind. Bereits im Juli 1995 hat der Bundesrat für den Bereich der EU europaweite Mindeststandards für Heim- und Telearbeit durch den Gesetzgeber gefordert und den Erlass einer entsprechenden EU-Richtlinie für notwendig erklärt[74]. Dies ist jedoch bis zum heutigen Tag nicht umgesetzt worden.

Dass dann, wenn Telearbeit über die nationalen Grenzen hinaus vereinbart wird, schwierige Probleme auftreten, zeigt ein Fall aus der Berliner Landesverwaltung.

> *Ein Beamter einer Landesbehörde wollte einen Teil seiner Arbeit in seiner Wohnung in einer niederländischen Stadt verrichten. Da die Behörde daran interessiert war, den Mitarbeiter nicht zu verlieren, fragte sie nach den datenschutzrechtlichen Voraussetzungen, insbesondere vor dem Hintergrund der Bestimmungen der europäischen Datenschutzrichtlinie zum Datenexport.*

Die entscheidende Frage war, ob diese Form der Heimarbeit nach Berliner Landesrecht abgewickelt werden konnte, so wie dies in anderen Fällen geschah, oder ob mit dem Transport bzw. der Übermittlung der Daten in die Niederlande nicht zusätzliche Vorschriften z. B. niederländisches Datenschutzrecht zu beachten sein würden.

In der Tat legt die *europäische Datenschutzrichtlinie* fest, dass dann, wenn in einem Mitgliedstaat eine Betriebsstätte eines Unternehmens besteht, das in einem anderen Staat seinen Sitz hat, das Recht des Mitgliedstaates gilt (Art. 4 EU-Richtlinie) – das würde bei entsprechender Anwendung im vorliegenden Fall bedeuten, dass der Arbeitsplatz des Mitarbeiters niederländischem Recht unterliegen würde, was jedenfalls im öffentlichen Bereich zu erheblichen Schwierigkeiten geführt hätte.

---

73 KOM (93) 700 endg.; Ratsdok. 11101/93
74 Beschluss vom 14. 7. 95, BR-Drs. 296/95

Wir haben die Auffassung vertreten, dass im vorliegenden Fall diese Regelung nicht gilt; der Heimarbeitsplatz, jedenfalls soweit er im Rahmen eines Dienstverhältnisses besteht, stellt keine eigene „Betriebsstätte“ dar, sondern einen Annex der Berliner Dienststelle ohne Auswirkung auf das Rechtsregime. In Anlehnung an die „Käseglockentheorie“ des Internationalen Privatrechts gilt hier ausschließlich deutsches Recht, natürlich einschließlich aller damit verbundenen Kontrollrechte.

Die niederländische Datenschutzbehörde Registratiekamer hat unsere Rechtsauffassung bestätigt, allerdings darauf hingewiesen, dass hinsichtlich der Datensicherungsvorschriften niederländisches Recht gilt – kein Schaden, da dieses eher strengere Anforderungen stellt als das deutsche.

3.3 Die ungeahnten Folgen eines fehlenden Fahrscheins

Die Probleme des *Outsourcing* sind von uns schon mehrfach in Jahresberichten erörtert worden[75]. In Berlin war 1998 die Auslagerung personenbezogener Datenverarbeitung in einem Bereich Gegenstand einer Prüfung, der von vielen als besonders sensibel bewertet wird – wohl deswegen, weil es jedem so leicht „passieren“ kann: Sowohl die Deutsche Bahn AG (DB) samt S-Bahn Berlin GmbH (S-Bahn) als auch die Berliner Verkehrsbetriebe (BVG) haben aus Gründen der Wirtschaftlichkeit die Verarbeitung der Daten von *Schwarzfahrern* fremden Dienstleistungsunternehmen übertragen.

Wird ein Fahrgast bei einer Kontrolle ohne gültigen Fahrausweis angetroffen, so wird dadurch ein langwieriges – dem Betroffenen nur in Bruchstücken offenbartes – Verfahren angestoßen, das nach unterschiedlichen Bestimmungen zu bewerten ist, je nachdem, wessen Beförderungsleistung in Anspruch genommen wurde. Alle drei Verkehrsbetriebe haben bestimmte Verfahrensweisen entwickelt, mit denen einerseits das (bei einer Schwarzfahrt fällige) erhöhte Beförderungsentgelt eingezogen werden soll *(Inkassoverfahren),* andererseits aber auch Wiederholungsfälle ermittelt werden können, bei denen das Verkehrsunternehmen über die strafrechtliche Verfolgung des „Mehrfachtäters“ befinden will. Die drei genannten Unternehmen haben bestimmte Aufgaben aus dem Gesamtkomplex unabhängig voneinander und mit jeweils eigenen Verträgen auf voneinander getrennte Firmen der INFOSCORE AG (Informationen, Forderungsmanagement, Scoringsysteme) in Rastatt/Baden-Württemberg ausgelagert: Die Credidata GmbH (Unternehmensbereich Treuhand und Verrechnung), die Süd-Westdeutsche Inkasso-KG (SWI, Unternehmensbereich Forderungseinzug) sowie die Infodata GmbH (Unternehmensbereich Information).

[75] JB 1993, 3.2; JB 1994, 3.3; JB 1997, 4.8.1

Die datenschutzrechtliche Zulässigkeit der einzelnen Verfahrensschritte ist bei DB und S-Bahn nach den Bestimmungen des Bundesdatenschutzgesetzes zu beurteilen, während für die Verfahrensweise der BVG (als Anstalt des öffentlichen Rechts) die speziellen Datenschutzbestimmungen der Verordnung über die Verarbeitung personenbezogener Daten bei den Berliner Verkehrsbetrieben (BVG) vom 30. Juni 1994 (BetriebeVO)[76] heranzuziehen sind.

BVG und S-Bahn haben nicht nur für die Beratung von Fahrgästen, sondern auch für die Fahrscheinkontrolle und die Erfassung von Personen ohne Fahrschein *private Wachschutzunternehmen* beauftragt. Da die Mitarbeiter nur genau festgelegte Datenverarbeitungsschritte und nicht weiter gehende Funktionen wahrnehmen, handelt es sich um Datenverarbeitung im Auftrag, die im Rahmen der Weisungen des Auftraggebers ohne weitere Voraussetzungen zulässig ist[77].

Während die BVG dieses Auftragsverhältnis und die damit einhergehenden Rechte und Pflichten des Auftragnehmers und des Auftraggebers in einem Vertrag festgehalten hat, war dies bei der S-Bahn zunächst nicht der Fall, obwohl ohne den Abschluss eines schriftlichen Vertrages ein Verstoß gegen § 11 BDSG vorliegt. In einem solchen Vertrag sind insbesondere der Umfang der Datenverarbeitung sowie die vom Auftragnehmer vorzunehmenden technischen und organisatorischen Maßnahmen festzulegen.

Nach der Eisenbahnverordnung (DB, S-Bahn) und den einschlägigen Tarifregelungen (BVG) hat das Verkehrsunternehmen einen Anspruch auf die Entrichtung eines erhöhten Beförderungsentgeltes, wenn der Fahrgast keinen gültigen Fahrausweis besitzt oder ihn bei einer Kontrolle nicht vorzeigen kann. Der Kontrolleur nimmt in diesem Fall die personenbezogenen Daten des „Schwarzfahrers“ in den dafür vorgesehenen Vordruck auf. Bei der BVG werden vorher die von dem Betroffenen angegebenen Personalien (wenn er kein Ausweispapier mitführt) telefonisch auf Übereinstimmung mit den Angaben im Melderegister des Landeseinwohneramts Berlin überprüft (§ 25 Meldegesetz).

Zweck der Datenerhebung ist einerseits die Beitreibung des erhöhten Beförderungsentgelts und zum anderen die Erfassung von Wiederholungsfällen (gegebenenfalls mit dem Ziel der Anzeigeerstattung wegen Beförderungserschleichung). Letzteres Interesse besteht auch dann, wenn der Schwarzfahrer das erhöhte Beförderungsentgelt sofort bar bezahlt. Rechtsgrundlage für die Datenverarbeitung der DB sowie der S-Bahn ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG, für die der BVG § 3 Abs. 1 der BetriebeVO.

[76] GVBl S. 229

[77] JB 1993, 3.2; zu den Abgrenzungsproblemen zwischen Datenverarbeitung im Auftrag und Funktionsübertragung vgl. JB 1997, 4.8.1

Nach dem Bundesdatenschutzgesetz ist das Speichern, Verändern oder Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Sowohl DB als auch S-Bahn haben ein berechtigtes (wirtschaftliches) Interesse daran, den ihnen jeweils zustehenden erhöhten Fahrpreis einzufordern. Sie haben auch ein berechtigtes Interesse daran, als Verletzte Strafanzeige zu erstatten. Ein überwiegendes schutzwürdiges Interesse des Betroffenen an dem Ausschluss dieser Datenspeicherung kann nicht anerkannt werden.

DB und S-Bahn geben jeweils die Daten an die Credidata GmbH weiter. Diese ist damit beauftragt, die Einsprüche der Betroffenen anzunehmen, wobei die Entscheidung hierüber bei den Einspruchsstellen des jeweiligen Verkehrsunternehmens bleibt. Die personenbezogenen Daten des Schwarzfahrers werden in einer Datei erfasst *(Mehrfachtäter-, Wiederholungstäter- oder Schwarzfahrerdatei),* die nach den vom Verkehrsbetrieb festgelegten Kriterien verwaltet werden. Credidata versendet standardisierte Mahnschreiben und überwacht einen eventuellen Zahlungseingang. Wegen des der Credidata GmbH auferlegten engen Handlungsrahmens sowie der fehlenden Entscheidungsbefugnis handelt es sich um Auftragsdatenverarbeitung, die keiner besonderen Befugnisnorm bedarf.

Die DB erwägt jedoch neuerdings, der Credidata eine umfassende Entscheidungsbefugnis hinsichtlich der Abwicklung des „Debitorenmahnverfahrens“ (mehrstufige Versendung von Mahnschreiben) einzuräumen. Anschließend sollen die Daten nach wie vor zur Durchführung des Inkassoverfahrens an die SWI übermittelt werden. Die Voraussetzungen, unter denen dieser weitere Schritt zulässig ist, sind noch in Diskussion, insbesondere deshalb, weil das berechtigte Interesse der DB an der Einschaltung eines weiteren Unternehmens nicht erkennbar ist.

Die BVG hat die Credidata GmbH nicht in das Verfahren eingebunden. Vielmehr gibt die BVG die Daten, nachdem sie selbst die ersten Mahnschreiben versandt und etwaige Zahlungseingänge geprüft hat, sogleich an das Inkassounternehmen SWI weiter. SWI führt für die BVG einerseits die Wiederholungstäterdatei und betreibt andererseits das Inkassoverfahren, sobald die BVG die Forderungen an die SWI abgetreten hat. Das Führen der Wiederholungstäterdatei, mit deren Hilfe die BVG entscheidet, gegen wen sie Strafanzeige wegen Beförderungserschleichung erstattet, stellt wiederum eine Auftragsdatenverarbeitung durch die SWI für die BVG dar. Die SWI hat sich diesbezüglich zur Einhaltung des Berliner Datenschutzgesetzes verpflichtet und sich insbesondere der Kontrolle durch den baden-württembergischen Landesdatenschutzbeauftragten unterworfen (§ 3 Abs. 4 BlnDSG).

In der *Inkassodatei* werden diejenigen Personen gespeichert, gegen die ein erhöhtes Beförderungsentgelt eingetrieben werden muss. Die SWI hält diese Datenbestände getrennt voneinander je nachdem, ob es sich um Kunden der DB, der S-Bahn oder der BVG handelt. Sie benötigt diese Daten zur eigenverantwortlichen Durchführung des Inkassoverfahrens, das bis zur gerichtlichen Geltendmachung der Forderung und bis zu ihrer Vollstreckung durch SWI reichen kann.

Bei der Übertragung des gesamten Inkassoverfahrens liegt keine bloße Auftragsdatenverarbeitung vor, sondern eine Funktionsübertragung. Dies hat zur Folge, dass die SWI als eigene Daten verarbeitende Stelle tätig wird und die Verantwortung für die Rechtmäßigkeit der Verarbeitung der bei ihr gespeicherten Daten selbst trägt. Zwar ist bei einer Funktionsübertragung – anders als bei der Auftragsdatenverarbeitung – ein schriftlicher Vertrag nicht obligatorisch. Diese eigenwillige gesetzliche Lücke muss jedoch durch entsprechende Maßnahmen ausgeglichen werden: Es ist dringlich anzuraten, Funktionsnehmern wie der SWI Vorgaben für den datenschutzrechtlichen Umgang mit den in seiner Verantwortung stehenden Daten zu machen, die das schutzwürdige Interesse des Einzelnen an der Rechtmäßigkeit der Verarbeitung seiner Daten berücksichtigen. Da es sich bei der SWI um eine eigene Daten verarbeitende Stelle (und nicht nur um einen unselbständigen Teil des Daten verarbeitenden Verkehrsbetriebes) handelt, hat sie bei der Tätigkeit als Inkassounternehmen das Bundesdatenschutzgesetz zu beachten und unterliegt diesbezüglich der Kontrolle durch das baden-württembergische Innenministerium als Aufsichtsbehörde.

Aus der rechtlichen Einordnung der SWI als Funktionsnehmerin folgt, dass die Weitergabe der bei dem jeweiligen Verkehrsbetrieb erhobenen Daten an die SWI eine Datenübermittlung darstellt, die (mangels Einwilligung des Betroffenen) nur zulässig ist, wenn eine Rechtsvorschrift sie erlaubt.

Die Übermittlungsbefugnis der BVG ergibt sich aus § 3 Abs. 2 BetriebeVO, nach dem die BVG berechtigt ist, die in Abs. 1 genannten Daten (u. a. Name, Anschrift, Geburtsdatum) zur Wahrnehmung ihrer Rechte an Dritte, insbesondere an Strafverfolgungsbehörden und die Inkassounternehmen, weiterzugeben, wobei die Weitergabe der Daten an Inkassounternehmen nur zur Forderungseinziehung erfolgen darf. Für die DB und die S-Bahn ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG einschlägig. Sofern ein zivilrechtlicher Anspruch besteht, haben alle Unternehmen das Recht, bestehende Forderungen, die der Betroffene trotz mehrerer Mahnungen nicht erfüllt hat, mit Hilfe eines Inkassounternehmens einziehen zu lassen.

Allerdings entstanden Zweifel, ob nicht deswegen doch schutzwürdige Interessen am Unterbleiben der Übermittlung bestehen, weil die SWI Daten an ein weiteres Unternehmen, nämlich die Infodata GmbH,

eine Auskunftei, weitergibt. Die *Datenübermittlungen an Auskunfteien* zur Überprüfung der Bonität ist nach § 28 Abs. 2 Satz 1 Nr. 1 a) BDSG dann zur Wahrung berechtigter Interessen Dritter, nämlich zum Schutz potenzieller Gläubiger des Betroffenen, gerechtfertigt, wenn es sich um gesicherte und beweisbare Daten handelt, die die Zuverlässigkeit des Betroffenen in Frage stellen, wie z. B. Zwangsvollstreckung, Konkurs, Haftbefehl, Abgabe der eidesstattlichen Versicherung nach § 807 ZPO, Pfändungen, Inanspruchnahme einer Lohnabtretung oder Wechsel- und Scheckproteste *(„harte Negativ-Merkmale").*

Die Nichtzahlung des erhöhten Beförderungsentgelts kann jedoch viele Gründe haben, die dem Inkassounternehmen nicht ohne weiteres bekannt sind, etwa Zahlungsunfähigkeit, Zahlungsunwilligkeit, aber auch das Bestreiten der Rechtmäßigkeit der Forderung, etwa weil der Betroffene im Besitz einer Jahreskarte ist oder weil er über die Auslegung sonstiger Tariffragen eine andere Meinung als der Verkehrsbetrieb vertritt. Die Übermittlung derartiger *weicher Negativ-Merkmale* kommt nur unter sehr engen Voraussetzungen in Betracht. Im Allgemeinen ist davon auszugehen, dass eine Übermittlung an eine Auskunftei dann möglich ist, wenn positiv festgestellt werden kann, dass das Verhalten des Betroffenen auf Zahlungsunwilligkeit bzw. Zahlungsunfähigkeit beruht. Um dies in Erfahrung zu bringen, muss das Inkassounternehmen dem Betroffenen vor der Übermittlung seiner Daten an Infodata Gelegenheit geben, Einwendungen gegen die Forderung zu erheben, und ihn darüber informieren, dass für den Fall, dass keine Einwendungen vorgetragen werden, die Übermittlung seiner Daten an die Auskunftei vorgesehen ist.

Ein derartiger Hinweis ist zwar auf den Mahnschreiben der SWI abgedruckt. Bei Verweigerung der Zahlung bzw. Nichtbeantwortung der Mahnschreiben erscheint jedoch zweifelhaft, ob daraus auf eine generelle Zahlungsunwilligkeit bzw. Zahlungsunfähigkeit geschlossen werden darf, was allein zur Übermittlung dieser Daten an die Auskunftei berechtigen würde: Die Bereitschaft, eine „normale Forderung" (etwa aus einem Kaufvertrag) zu begleichen, ist ungleich höher als bei der Bezahlung eines erhöhten Beförderungsentgelts. SWI darf deshalb nur harte Negativ-Merkmale an die Auskunftei übermitteln.

Wir haben DB und S-Bahn aufgefordert, die SWI zu verpflichten, keine weichen Negativ-Merkmale weiterzugeben. Die S-Bahn ist unserer Empfehlung nicht gefolgt mit der Folge, dass SWI die Daten an die Auskunftei schon dann übermittelt, wenn der Schuldner auf den entsprechenden Hinweis und die Mahnung nicht reagiert. Die DB hat dagegen zugesagt, SWI vertraglich zu verpflichten, die Auskunftei nur bei Forderungen ab 50,00 DM dann zu informieren, wenn keinerlei Reaktion des Schuldners auf die insgesamt fünf Mahnungen erfolgt ist oder wenn der Schuldner gerichtlich verurteilt worden ist. Die von der BVG an SWI übermittelten Daten werden in keinem Fall an die Auskunftei weitergegeben.

Die Auskunftei Infodata darf ihrerseits Bonitätsdaten über einen Schuldner an Credidata bzw. SWI übermitteln, damit diese feststellen können, ob der Betroffene bereits als Schuldner geführt wird und deshalb Maßnahmen zum *Forderungseinzug* lohnenswert sind. Voraussetzung ist, dass der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegt und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 29 Abs. 2 Satz 1 BDSG). Aus Sicht der DB und der S-Bahn (bzw. der beauftragten Unternehmen Credidata und SWI) besteht ein berechtigtes Interesse daran zu wissen, ob eine bestimmte Person insolvent ist und das Unternehmen deshalb keinen weiteren finanziellen Aufwand zur Einziehung einer Forderung betreiben muss. Dem steht ein schutzwürdiges Interesse des Betroffenen nicht entgegen.

Von großer Bedeutung für die Betroffenen ist natürlich die Frage, *wie lange die Daten gespeichert werden.*

Bei der BVG sind die zur Beitreibung des erhöhten Beförderungsentgelts sowie zur Erfassung von Wiederholungsfällen erhobenen Daten ein Jahr nach der Abwicklung der auf den Vorfall gegründeten Rechtswirkungen, spätestens zwei Jahre nach dem letzten einschlägigen Vorfall zu löschen (§ 3 Abs. 4 BetriebeVO). Dies bedeutet, dass die Daten des „Ersttäters" nur ein Jahr gespeichert werden dürfen, es sei denn, es wird innerhalb dieses Jahres eine weitere Schwarzfahrt entdeckt. Dann erhöht sich die Speicherfrist auch für die erste Schwarzfahrt auf zwei Jahre, beginnend ab dem Tag der zweiten Schwarzfahrt. Entgegen dieser eindeutigen Bestimmung speichern BVG und SWI die Daten des „Ersttäters" auch ohne Wiederholungsfall für zwei Jahre. Eine hinreichende Begründung dafür konnte die BVG nicht abgeben. Wir halten diese Verfahrensweise für rechtswidrig.

Bei *Kindern* zwischen sechs und vierzehn Jahren erfolgt die Löschung nach Zahlung des erhöhten Beförderungsentgelts (§ 3 Abs. 4 Betriebe VO). Diese Regelung trägt dem Umstand Rechnung, dass die Daten von Minderjährigen (unter 14 Jahren) nach Zahlung des erhöhten Beförderungsentgelts nicht mehr erforderlich sind, weil nicht nur die zivilrechtliche Verfolgung der Vorgangs ausscheidet, sondern wegen Strafunmündigkeit auch die strafrechtliche, so dass die Daten auch nicht in die „Wiederholungstäterdatei" aufzunehmen sind. Wir haben auch der DB und der S-Bahn eine entsprechende Verfahrensweise empfohlen.

Die Speicherdauer bei den Vorgängen der DB beträgt grundsätzlich ein Jahr, das bei einem Wiederholungsfall erneut zu laufen beginnt, maximal jedoch drei Jahre. Bedenken gegenüber dieser Speicherfrist bestehen nicht, da das Unternehmen drei Jahre lang die Beförderungserschleichung strafrechtlich verfolgen lassen kann (§ 78 Abs. 2 Nr. 5 Strafgesetzbuch), andererseits aber nicht verfolgen lässt, wenn der Betroffene innerhalb eines Jahres nicht nochmals auffällt. Insofern ist die Kenntnis der Daten für diese Zeiträume erforderlich im Sinne des

§ 35 Abs. 2 Nr. 3 BDSG. Da diese drei Jahre die Höchstfrist für jeden einzelnen Vorfall darstellen, sind diese Speicherfristen günstiger ausgestaltet als bei der BVG, bei der bei alljährlichen Wiederholungsfällen die Löschung auch der allerersten Schwarzfahrt (die für sich z. B. schon drei Jahre zurückliegt und eigentlich schon hätte gelöscht werden müssen) erst zwei Jahre nach dem letzten einschlägigen (z. B. zehnten) Vorfall erfolgen muss. Am kürzesten sind die Speicherfristen bei den Vorgängen der S-Bahn. Die Daten werden ein Jahr nach ihrer Erfassung gelöscht.

Es kommt häufiger vor, dass Schwarzfahrer bei Kontrollen angeben, sie hätten keine Ausweispapiere dabei, und die Personalien anderer Personen nennen – oder sie geben zwar die richtigen Personalien an, streiten aber hinterher ab, selbst kontrolliert worden zu sein. Da eine Pflicht zum Mitführen eines Ausweisdokuments nicht besteht, kann die Identität des Schwarzfahrers nicht vor Ort geprüft werden.

Von der DB wurden derartige Fälle bislang ebenfalls in die Schwarzfahrerdatei aufgenommen mit der Begründung, dass diese Fallkonstellationen sehr häufig unter Jugendlichen auftreten, die bei einer Konfrontation mit verschiedenen Verdachtsfällen einräumen, dass sie in Wahrheit selbst mehrfach schwarzgefahren seien (aber ihre Identität verschleiern wollten). Wir haben die DB darauf hingewiesen, dass die Speicherung von Personen, bei denen sich erst später herausstellt, ob sie Täter oder Opfer gewesen sind, in der Schwarzfahrerdatei selbst nicht zulässig ist, weil die Speicherung dieser Daten mit dem Zweck der Datei nicht übereinstimmt. Die Speicherung ihrer Daten in der „Schwarzfahrerdatei" ist nicht geeignet, die Verdachtsperson oder das Opfer – dem Zweck der Datei entsprechend – als Täter „im wiederholten Fall" zu identifizieren. Die DB hat sich zwischenzeitlich dieser Auffassung angeschlossen und das Verfahren dahingehend geändert, dass künftig bei Abstreiten der Identität sofort Strafanzeige (ggf. gegen unbekannt) erstattet wird. Die Speicherung erfolgt nur noch mit ausdrücklicher Einwilligung des Betroffenen, nachdem er um Unterstützung bei der Sachverhaltsaufklärung gebeten worden ist.

Bei der S-Bahn werden seit neuestem alle Fälle des *Personalienmissbrauchs* (mit Namen, Vornamen, Geburtsdatum) in einer gesonderten Datei gespeichert. Bei einer Kontrolle werden die Angaben des Betroffenen in ein Handterminal eingegeben. Das Gerät signalisiert lediglich, ob die Angaben in dieser Datei erfasst sind, nicht jedoch wird die Datei mit allen bereits missbrauchten Namen sichtbar. Zeigt das Gerät an, dass die Angaben bereits missbraucht wurden, wird der Bundesgrenzschutz zur *Klärung der Identität* des Betroffenen hinzugezogen. Diese Datei wird also zu einem anderen Zweck geführt als die Mehrfachtäterdatei, nämlich mit dem Ziel, bereits vor Ort diejenigen Fälle aufzuklären, in denen ein Schwarzfahrer die Personalien einer anderen Person missbraucht. Eine Veränderung bereits eingegebener Daten kann durch

den Kontrolleur nicht erfolgen. Bei fehlerhafter Eingabe bedeutet dies, dass – mangels Löschungsmöglichkeit – nur ein Vermerk angebracht werden kann. Beim Einlesen in die Datei wird der Datensatz automatisch (und unwiederbringlich) gelöscht und gleichzeitig ein Schreiben an den Kunden mit der entsprechenden Information erstellt. Falls der Betroffene später geltend macht, nicht der wahre Schwarzfahrer zu sein, wird ihm eine entsprechende eidesstattliche Erklärung (mit dem Hinweis auf die Strafbarkeit einer falschen Erklärung) abverlangt. Sodann wird der Datensatz in der Mehrfachtäterdatei mit der Angabe „Adressmissbrauch" gesperrt und in eine *Namensmissbrauchsliste* übernommen. Wir haben der S-Bahn empfohlen, eine Speicherung in der Namensliste – mangels Rechtsgrundlage – nur mit Einwilligung des Betroffenen vorzunehmen.

Auch die BVG führt eine interne Datei, die die Namen und Geburtsdaten von Fahrgästen enthält, für die bereits ein Namensmissbrauch vorgelegen hat. Werden die angegebenen Daten bei einer telefonischen Nachfrage in der Datenbank gefunden, so wird die Polizei zur Identitätsprüfung hinzugezogen. Die Übernahme der Daten in diese Namensmissbrauchsdatei darf nur mit Einwilligung des Betroffenen erfolgen, weil auch für die BVG eine Rechtsgrundlage für die Verarbeitung der Daten der Namensmissbrauchsopfer nicht existiert. Entgegen unserer Empfehlung speichert die BVG die Daten jedoch auch ohne Einwilligung des Betroffenen.

3.4 Jagdfieber im Internet

Das Internet bekommt in der Öffentlichkeit zunehmend den Ruf, Umschlagplatz für *Kinderpornografie* oder rechtsradikale Propaganda zu sein. Rassistische Texte und kinderpornografische Darstellungen dürfen in Deutschland weder hergestellt noch verbreitet werden. Dieses gilt auch für neue technische Hilfsmittel wie das Internet. Dies fordert natürlich zunehmend die Strafverfolgungsbehörden und Gerichte, sich mit der neuen Materie zu beschäftigen. Die Strafverfolgungsbehörden gehen verstärkt dazu über, „Online-Delikte" aufzuspüren und zu bekämpfen. Im Bundeskriminalamt, wo die „Zentralstelle zur Bekämpfung der Internetkriminalität" ihre Arbeit aufgenommen hat, sollen 20 Bedienstete anlassunabhängig nach strafrechtlich relevantem Material im Internet und Online-Diensten recherchieren (Initiativermittlungen). Im Bayerischen Landeskriminalamt gehen schon seit 1995 Beamte im Netz Streife. In Berlin ist dies auch geplant.

Gegen das Aufspüren von Verbrechen im Netz durch *„Cyber patrols"* bestehen grundsätzlich keine Bedenken. Das betrifft insbesondere die Überwachung des Internet bezüglich allgemein zugänglicher Informationen. Recherchen unter einer Legende oder unter Vortäuschung der Identität sind jedoch nur bei Vorliegen der Voraussetzungen in der StPO oder den Polizeigesetzen der Länder zulässig. Hier gelten im Internet keine anderen Bedingungen als im nicht „virtuellen Leben".

Wie problematisch die Strafverfolgung von „Online-Delikten“ sein kann, zeigt das Urteil gegen den ehemaligen Geschäftsführer des Internet Providers *CompuServe* Information Services GmbH[78]. Ihm wurde vorgeworfen, gemeinschaftlich mit der „Mutterfirma“ CompuServe Incorporated in den USA den Kunden von CompuServe in Deutschland, die auf dem News-Server[79] von CompuServe USA bereitgehaltenen gewalt-, kinder- und tierpornografischen Darstellungen zugänglich gemacht zu haben. Bereits 1995 war die Polizei auf CompuServe aufmerksam gemacht worden. Sie leitete Verfahren gegen mehrere CompuServe-Kunden ein, die kinderpornografische Bilder in Newsgroups zur Verfügung gestellt hatten. Rund 2½ Jahre später wurde der Geschäftsführer von CompuServe in Deutschland zu einer zweijährigen Haftstrafe auf Bewährung verurteilt, da er die Verbreitung von gewalt-, kinder- und tierpornografischen Bildern in Newsgroups nicht unterbunden hat.

Mit der Verabschiedung des *Teledienstegesetzes* (TDG) als Teil des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) im Juli 1997[80] wurden *Verantwortlichkeiten von Diensteanbietern* geregelt. Danach sind Diensteanbieter für fremde Inhalte nicht verantwortlich, wenn sie lediglich den Zugang zur Nutzung vermitteln (§ 5 Abs. 3 TDG). Diensteanbieter sind nur dann für fremde Inhalte, die sie zur Nutzung bereithalten, verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und ihnen es technisch möglich und zumutbar ist, deren Nutzung zu verhindern (§ 5 Abs. 2 TDG).

Die in § 5 Abs. 2 TDG vorausgesetzte Kenntnis von Inhalten, die die Verantwortung für fremde Inhalte festlegt, wirft ein generelles Problem auf. Ein Internet Provider kann nicht verpflichtet sein, das Netz nach strafbaren Inhalten zu durchsuchen. Dieses könnte sogar strafbar sein: § 5 Abs. 4 TDG bestimmt, dass ein Diensteanbieter verpflichtet ist, die Nutzung rechtswidriger Inhalte zu sperren, wenn er unter Wahrung des Fernmeldegeheimnisses nach § 85 Telekommunikationsgesetz von diesen Inhalten Kenntnis erlangt. D. h., das Fernmeldegeheimnis muss auf jeden Fall gewahrt werden, ein Mitlesen fremder E-Mails zum „Aufspüren“ von strafbaren Inhalten ist unzulässig und nach § 206 Strafgesetzbuch strafbar. Eine Verpflichtung zur Sperrung kann daher nur dann bestehen, wenn der Diensteanbieter von der Verbreitung strafbarer Inhalte positiv Kenntnis hat. Eine positive Kenntnis liegt z. B. dann vor, wenn ihn die Strafverfolgungsbehörden in Kenntnis gesetzt haben.

Im Fall CompuServe war problematisch, dass die Informationen auf einem Rechner in den USA gespeichert waren und die CompuServe-Nutzer in Deutschland über eine Standleitung in die USA darauf zugreifen konnten. Dies bedeutet, dass Filterprogramme, die die Sperrung bestimmter Newsgroups ermöglichen, auf dem Rechner in den USA installiert sein müssten. Im Fall der USA wäre dieses noch denkbar. In anderen Ländern, in denen die aufgezählten Tatbestände nicht strafbar sind, lassen sich Inhalte, die in diesen Ländern in das Netz eingespeist werden, von Deutschland aus nicht kontrollieren. Sicherlich kann man durch Sperrung bestimmter Newsgroups oder WWW-Adressen bei Internet-Providern in Deutschland den direkten Zugang zu den Informationen erschweren, verhindern kann man ihn dagegen nicht. Die Vergangenheit hat gezeigt, dass derart „zensierte“ Inhalte sehr schnell an anderen Stellen im Internet in Form von Kopien wieder auftauchten.

Die Aktivitäten der Strafverfolgungsbehörden sollten sich daher nicht gegen die Provider richten, sondern gegen die Kriminellen selbst. Die Aufklärung und Bekämpfung von Straftaten im Internet ist dringend notwendig. Dazu gehört neben der gezielten Ausbildung der Strafverfolger auf dem Gebiet moderner Informations- und Kommunikationstechnik auch eine ausreichende technische Austattung.

Über die Strafverfolgung im Internet hinaus hat die Polizei das Internet auch zu Fahndungszwecken entdeckt. Auch beim Berliner LKA bestehen derartige Planungen. Die neuartigen Medien, wie z. B. das World Wide Web (WWW), bieten ideale Möglichkeiten, bei Fahndungen relevante Informationen weltweit in kürzester Zeit zur Verfügung zu stellen. Doch bei dieser Nutzungsart entstehen sowohl rechtliche als auch sicherheitstechnische Problemfelder. Eine *Fahndung über das Internet* ist zugleich Öffentlichkeitsfahndung und internationale Fahndung. Beide Kriterien beeinflussen die Zulässigkeit der Nutzung des Internet als Fahndungsmittel.

Der „Steckbriefparagraf“ § 131 StPO ist keine hinreichende Rechtsgrundlage, auf die diese neuartige und tief in das Persönlichkeitsrecht eingreifende Fahndungsmethode gestützt werden kann. Der Entwurf des Strafverfahrensänderungsgesetzes 1996 (StVÄG 1996)[81] und der von der neuen Justizministerin vorgelegte StVÄG-Entwurf 1999[82] regeln lediglich die Fahndung mittels Aufruf an die Öffentlichkeit. Eine Rechtsgrundlage für die internationale Fahndung oder gar eine Fahndung durch das Internet ist nicht geplant. Die Veröffentlichung eines „Steckbriefes“ im Internet ist jedoch, da der Zugriff nicht beschränkt werden kann, ein weltweiter Fahndungsaufruf und besitzt damit eine ganz andere Qualität als eine nationale oder örtliche Fahndung.

Auch aus sicherheitstechnischer Sicht wirft die Öffentlichkeitsfahndung im Internet erhebliche Probleme auf. Grundsätzlich muss berücksichtigt werden, dass Informationen, die in das WWW eingestellt werden, zum Zwecke der Verbreitung eingestellt werden und nicht rückholbar sind. Es können beliebig viele Kopien erstellt werden. Der originale

78 Urteil des AG München vom 28. Mai 1998 – 8340 Ds 465 Js 173158/95
79 Rechner, auf dem öffentliche Nachrichten im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) zum Abruf bereitgehalten werden
80 BGBl. I, S. 1870
81 BR-Drs. 961/96
82 BR-Drs. 65/99

Fahndungsaufruf auf einem WWW-Server der Polizei kann zwar gelöscht werden, auf mögliche Kopien dieses Fahndungsaufrufes im Internet hat das jedoch keine Auswirkung.

Die WWW-Server der Polizei und damit die auf diesen Servern veröffentlichten Fahndungsaufrufe müssen durch Anwendung von Zugriffsschutzmechanismen und Sicherheitsinfrastrukturen gegen unbefugte Manipulation geschützt werden. Durch den Einsatz kryptografischer Verfahren, wie z. B. digitale Signaturen und digitale Wasserzeichen, kann eine Veränderung der veröffentlichten Informationen nachweisbar gemacht werden. Zurzeit existiert die zur Überprüfung durch die Benutzer notwendige Infrastruktur jedoch noch nicht.

Ein weiteres Problem stellt eine Veröffentlichung von manipulierten oder gänzlich falschen Fahndungsaufrufen unter Vortäuschung einer Internet-Adresse der Polizei dar. Eine einfache Methode ist z. B. die Reservierung eines offiziell klingenden Domainnamen, wie z. B. http://www.berlin.lka.de durch eine Nicht-Polizeistelle und anschließendes Veröffentlichen der manipulierten Fahndungsaufrufe. Darüber hinaus gibt es eine Reihe von technischen Möglichkeiten vorzutäuschen, dass Daten von einem Polizei-Server stammen. Dieses kann z. B. durch Manipulation einer bestehenden Internet-Kommunikation, von Domain Name Servern (DNS), Dienstleistungsprogrammen (Proxies) und lokalen Zwischenspeichern (Caches) erreicht werden.

Vor dem Hintergrund der dargestellten rechtlichen und sicherheitstechnischen Probleme sollte auf eine Personenfahndung im Internet derzeit verzichtet werden[83]. Auch bei Schaffung entsprechender Rechtsgrundlagen ist eine Öffentlichkeitsfahndung im Internet äußerst fragwürdig, da hier die Gefahr schwerwiegender Eingriffe in das Persönlichkeitsrecht besteht.

Nochmals: Kinderpornografie im Internet

Im Jahresbericht 1997 hatten wir über den Fall eines Arztes an einem Universitätsklinikum berichtet, gegen den wegen des Verdachts ermittelt wurde, über seinen privaten Computer unter Nutzung des von der Hochschule zur Verfügung gestellten Internetzuganges Bilder und Videos mit Kinderpornografie im Internet verbreitet zu haben[84]. Wie der Tagespresse zu entnehmen war, ist der Beschuldigte unterdessen wegen des Besitzes und der Verbreitung von Kinderpornografie zu zwei Jahren Freiheitsstrafe ohne Bewährung verurteilt worden.

Auch die neue Bundesregierung misst der Bekämpfung der Kinderpornografie im Internet große Bedeutung zu. In einer Antwort auf eine Kleine Anfrage im Bundestag führt die Bundesregierung dazu aus, dass

83 vgl. auch Budapest-Berlin-Memorandum vom 19. November 1996 der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation, JB 1996, Anlage 5.1
84 vgl. Jahresbericht 1997, 4.7.2

zur Bekämpfung der Kinderpornografie – wie auch in anderen Deliktsbereichen – die „. . . effektive internationale Zusammenarbeit der Ermittlungsbehörden zwingend erforderlich . . .“ ist[85]. Nach Auffassung der Bundesregierung ist gegenwärtig das wichtigste Mittel der internationalen Zusammenarbeit auf europäischer Ebene die geplante Europäische Polizeibehörde *Europol,* deren Mandat auch die Bekämpfung der Erzeugung, des Verkaufs und der Verbreitung von kinderpornografischem Material umfasse. Europol soll in diesem Bereich eine Zentralstellenfunktion ausüben, insbesondere aber „. . . zentrale Dateien mit personenbezogenen Daten führen können“. Die Bundesregierung befürwortet eine schnelle Aufnahme der Tätigkeit der Behörde.

Darüber hinaus soll im Zusammenhang mit der Evaluierung des Informations- und Kommunikationsdienste-Gesetzes[86] auch geprüft werden, ob unter dem Aspekt der Bekämpfung der Kinderpornografie künftig weitergehende Auskunfts-, (Mindest-)Speicherungs- und Identitätskontrollpflichten von Internetprovidern eingeführt werden sollen. Derartige Bestrebungen waren bereits im Gesetzgebungsverfahren zum IuKDG von den Datenschutzbeauftragten vehement kritisiert worden, eine im ursprünglichen Entwurf des IuKDG enthaltene Vorschrift war daraufhin im Verlauf des Gesetzgebungsverfahrens wieder gestrichen worden.

Initiative „Jugendschutz.net“

Die Verbreitung gefährdender und illegaler Inhalte im Internet hat die Jugendminister der Länder auf den Plan gerufen, auf deren Initiative hin zur Durchsetzung der geltenden Jugendschutzbestimmungen im Bereich der Mediendienste eine in Rheinland-Pfalz eingerichtete Stelle namens „Jugendschutz.net“ ins Leben gerufen wurde. „Jugendschutz.net“ prüft mittels entsprechender Software Internetangebote auf gefährdende Inhalte. Die verwendete Software kontrolliert Bilder, Texte oder Videos auf bereits indizierte Inhalte. Die Anbieter dieser Inhalte werden unter Androhung von Bußgeldern oder – beim Vorliegen von Straftaten – durch Hinzuziehung der Staatsanwaltschaft angehalten, derartige Inhalte zu löschen oder entsprechend Sperren einzurichten[87]. Dabei erhebt und speichert „Jugendschutz.net“ auch personenbezogene Daten der Anbieter. Die Verarbeitung dieser personenbezogenen Daten wird noch durch den Landesbeauftragten für den Datenschutz Rheinland-Pfalz kontrolliert.

3.5 Biometrie – Sesam öffne dich?

1983: Der James-Bond-Film „Sag niemals nie“ flimmert weltweit über die Leinwände der Kinos: Am Auge eines durch seine Drogensucht

85 BT-Drs. 14/35, S. 8
86 vgl. 5.3
87 vgl. BT-Drs. 13/11450 vom 28. 9. 1998, S. 1 f.

erpressbar gewordenen Offiziers der US Air Force wird eine „Hornhauttransplantation" vorgenommen, um den per Augenscanning realisierten Zugriffsschutz für den Austausch von Gefechtsattrappen durch Nuklearsprengköpfe zu überlisten. Diese Befugnis ist nämlich einzig dem amerikanischen Präsidenten vorbehalten und so ist das Transplantat folgerichtig eine „Nachbildung" dessen Auges.

Alles nur „Kintopp"?

1998: Olympische Winterspiele im japanischen Nagano: Die Biathleten gelangen nur dann in die Waffenkammer und damit an die zu ihrer Disziplin notwendigen – in falschen Händen durchaus gefährlichen – Sportgeräte, wenn das biometrische Muster ihrer Iris/Regenbogenhaut mit dem zuvor individuell gespeicherten Referenzmuster übereinstimmt. Was in dem zuvor erwähnten Film noch als Fiktion erscheinen mochte, ist Realität geworden.

Biometrie – was ist das eigentlich?

Lexikalisch wird die Biometrie als Lehre von der Anwendung mathematischer (statistischer) Methoden auf die Mess- und Zahlenverhältnisse der Lebewesen und ihrer Einzelteile definiert. Im engeren, auf die Computerwelt bezogenen Sinne ist dieser Begriff ein Synonym für den *Identitätsnachweis* von Personen unter Verwendung ihrer individuellen körperlichen Merkmale. Diese Merkmale müssen allerdings so einzigartig sein, dass sie möglichst nur einer einzigen Person eindeutig zugeordnet werden können. Selbst eineiige Zwillinge sollten von einem ausgefeilten, einem dem menschlichen Unterscheidungsvermögen überlegenen biometrischen Verfahren als unverwechselbare Individuen erkannt werden können. Womöglich störende „Accessoires" (z. B. Brillen, Toupets, Bärte) sollten auf geeignete Weise eliminiert werden können.

Zu einem solchen Verfahren gehören in der Regel drei wesentliche Komponenten:

- Zur Erfassung individueller biologischer Merkmale dienen technische Einrichtungen wie Sensoren oder Scanner.
- Die erfassten Daten sind unter Einsatz mathematischer/statistischer Methoden so zu abstrahieren, dass von den wesentlichen Merkmalen Referenzmuster abgespeichert werden können.
- Die dritte wesentliche Komponente ist der programmtechnisch umzusetzende Vergleichsalgorithmus.

Aus der Art der für ein biometrisches Verfahren genutzten Merkmale kann man eine Zweiteilung der Verfahren ableiten:

- Statische Verfahren, basierend auf physiologischen Merkmalen, die unveränderlich sind: Fingerabdruck, Hand- und Venengeometrie, Augenmerkmale (Netzhaut, Regenbogenhaut), Gesichtserkennung (visuell, thermisch), der gesamte Körper,
- Dynamische Verfahren, basierend auf verhaltenstypischen Merkmalen, die u. U. veränderlich sein können: Stimme, Motorik (Unterschrift, Tastenanschlag, Lippenbewegung).

Eine dritte Gruppe von Verfahren setzt Eingriffe in den Körper der Betroffenen voraus, wie z. B. die Blutbild- oder die DNA-Analyse. Da diese Verfahren zu Kontrollzwecken nicht geeignet sind, werden sie hier nicht behandelt.

Einige Verfahren sind lange eingeführt, andere Techniken haben die experimentelle Phase verlassen, sind auf dem Markt verfügbar und werden bereits intensiv genutzt. Dabei erweisen sich solche Verfahren als besonders erfolgreich, die zum einen hohen Sicherheitsstandards genügen (insbesondere beeinflusst durch die Invarianz und die Einzigartigkeit der zugrunde liegenden biometrischen Merkmale), sowie ein günstiges Kosten-Nutzen-Verhältnis aufweisen (geringer Erfassungs- und Verifikationsaufwand) und bei den Betroffenen ohne psychologische Hemmungen akzeptiert werden.

Fingerabdruck-Verfahren sind weit verbreitet, kostengünstig und hinreichend sicher. Sie sind abgeleitet aus dem seit über 100 Jahren bekannten daktyloskopischen Verfahren im polizeilichen Erkennungsdienst.

Handgeometrie-Verfahren werden zwar auch kostengünstig angeboten, gewährleisten allerdings nur eingeschränkte Sicherheit, da es hier zu viele Ähnlichkeiten bei unterschiedlichen Individuen gibt. Dafür gibt es kaum Akzeptanzprobleme, sieht man einmal von Einwänden aus hygienischen Gründen ab.

Verfahren, die auf der *Auswertung von Augenmerkmalen* beruhen, befriedigen zwar hohe Sicherheitsbedürfnisse, sind aber mit hohem Kostenaufwand verbunden und werden wegen des zur Merkmalserfassung benutzten (ungefährlichen) Laserstrahls nicht vorbehaltlos akzeptiert.

Gesichtserkennungs-Verfahren gewinnen aufgrund der geringen Akzeptanzprobleme – der Vergleich mit dem Fotografieren liegt nahe – in jüngster Zeit größere Bedeutung. Hier liegen die Probleme bei der Reduzierbarkeit der erfassten Merkmale auf Dateigrößen, die von preisgünstigen Geräten zu bewältigen wären.

Dynamische Verfahren, die sich auf den Vergleich von Verhaltensmerkmalen stützen, haben ebenfalls bereits Marktreife erlangt, sind allerdings wegen des meist damit verbundenen Zeitaufwands nicht derart universell einsetzbar (z. B. zur Zutrittskontrolle) wie die zuvor erwähnten statischen Verfahren.

Gesteigerten Sicherheitsbedürfnissen kommt man zunehmend durch sog. *Hybridverfahren* entgegen, d. h. solche Verfahren, bei denen eine Kombination verschiedener biometrischer Merkmale zum Vergleich herangezogen wird.

Bisher waren die Verfahren hinsichtlich der verwendeten Geräte (Hardware) und der damit verbundenen Verifikationsprozesse (Software) in hohem Maße herstellerabhängig (proprietär). Wie die derzeitige Entwicklung zeigt, bemüht man sich verstärkt darum, standardisierte Schnittstellen zu definieren, die es ermöglichen, Hard- und Software unterschiedlicher Hersteller zu kombinieren. Dies dürfte einen zunehmenden Einsatz biometrischer Systeme zur Folge haben.

Sinn des Einsatzes

Biometrische Verfahren erhalten zunehmende Bedeutung für *Kontrollsysteme,* mit deren Hilfe zwischen berechtigten und unberechtigten Personen unterschieden werden kann. Den bisher üblichen Kontrollsystemen liegen zumeist zwei Komponenten zugrunde. Das eine Element ist der Besitz des Sicherungsmechanismus, wie Schlüssel, Ausweise sowie Magnetstreifen- oder Chipkarten. Die zweite Komponente besteht im Wissen um ein individuell festgelegtes Geheimnis: Im Zahlungsverkehr als PIN, in der Datenverarbeitung als Passwort geläufig. Neben dem möglicherweise unangenehmen Verlust dieses Wissens durch Vergessen – der Geldautomat verweigert die Ausgabe dringend benötigten Bargeldes – weisen die beiden Kontrollelemente aber eine wesentlich unangenehmere Eigenschaft auf: Sie sind – gewollt oder ungewollt – übertragbar. Das hat zur Folge, dass jede Person, die über Besitz oder Wissen verfügt, davon auch Gebrauch machen kann, mithin zur Benutzung eines zu schützenden Systems autorisiert wird.

Erst durch die Kombination einer oder beider Komponenten mit einem nicht übertragbaren, eindeutig zuordenbaren persönlichen Kennzeichen erreichen Berechtigungsprüfungen eine neue Qualität: Aus der Autorisierung wird die *Authentifizierung,* d. h. es kann geprüft werden, ob der „Berechtigte“ auch tatsächlich die Person ist, für die sie sich ausgibt. Das Missbrauchsrisiko wird also ganz erheblich gemindert werden. Biometrische Verfahren können dies leisten.

Jedoch: „Wo Licht ist, ist auch Schatten“. Durch den Einsatz biometrischer Verfahren entstehen neue datenschutzrechtliche *Risiken.* Die abgespeicherten Referenzdaten können zu Zwecken genutzt werden, die über die Authentifizierung hinausgehen. Beispielsweise kann in einer zentralen Datenbank, in der die Referenzdaten abgelegt wurden, nicht nur überprüft werden, ob eine Person zu einer Gruppe von – dem System bekannten – Berechtigten gehört („one-to-one“), sondern es besteht auch die Möglichkeit, eine zunächst unbekannte Person mit Hilfe der gleichen Datenbank zu identifizieren („one-to-many“).

Auch für diese Art der Nutzung biometrischer Verfahren gibt es bereits praktische Anwendungen: In Großbritannien haben *Videoüberwachungssysteme* geradezu Hochkonjunktur und werden teilweise bereits flächendeckend zur Beobachtung öffentlicher Plätze, ja ganzer Städte eingesetzt. Mit Hilfe hochauflösender Videokameras, die eine

digitalisierte Aufzeichnung der von der Kamera erfassten Bilder ermöglichen, werden die Gesichtsmerkmale einzelner Personen derart aufbereitet, dass sie mit den durch ein biometrisches Gesichtserkennungs-Verfahren gewonnenen und in einer zentralen Datenbank gespeicherten Referenzmustern verglichen werden können, um unliebsame Zeitgenossen zu identifizieren und gegebenenfalls entsprechende Maßnahmen einzuleiten.

Biometrische Verfahren sind daher datenschutzrechtlich sehr zwiespältig zu beurteilen. Einerseits verletzt ihr Einsatz die informationelle Selbstbestimmung der Betroffenen, wenn deren biometrische Merkmale hinter ihrem Rücken mit denen gesuchter Personen verglichen oder für spätere Kontrollzwecke auf Vorrat registriert werden. Andererseits lassen sie wesentlich sicherere Authentifikationsverfahren erhoffen, damit die informationelle Selbstbestimmung durch die Verhinderung unbefugter Datenzugriffe geschützt wird.

Es muss also auf die *unbedingte Zweckbindung* der durch biometrische Verfahren gewonnenen personenbezogenen Daten geachtet werden. Im Sinne des Einsatzes datenschutzfreundlicher Technologien bei der Verarbeitung personenbezogener Daten sind in jüngster Zeit auch bei der Entwicklung von biometrischen Kontrollsystemen Tendenzen erkennbar, die diesem Anliegen Rechnung tragen. So werden mittlerweile solche Systeme auf dem Markt angeboten, die sich von zentral vorgehaltenen Datenbanken lösen und die Verfügungsgewalt über die persönlichen biometrischen Merkmale beim Betroffenen belassen.

Als ein dazu geeignetes Medium hat sich beispielsweise die *Chipkarte* erwiesen. Zum einen kann durch geeignete Maßnahmen bei der Erstellung von Referenzmustern und deren Speicherung (Einwegverschlüsselung, hinreichend kleine Dimensionierung) auf dem Chip verhindert werden, dass diese Daten selbst dann wieder auf ihren Ursprung zurückgeführt werden können, wenn die Karte in falsche Hände gelangt. Zum anderen weisen die mittlerweile entwickelten Chips eine so hohe Funktionalität auf, dass sie es gestatten, auch die Verifizierungsalgorithmen auf dem Chip zu implementieren. Eine geeignete „Versiegelung“ der Chipkarten sollte zudem böswillige Angriffe auf den Chip verhindern.

Es ist davon auszugehen, dass insbesondere die zuletzt beschriebene Entwicklung dazu beitragen wird, die Akzeptanz biometrischer Kontrollsysteme bei den Betroffenen zu erhöhen, auch – oder gerade weil – auf diese Weise die datenschutzrechtlichen Bedenken gegen deren Einsatz wesentlich reduziert werden können.

3.6 Der schwere Stand der behördlichen Datenschutzbeauftragten

Für die Anpassung der deutschen Datenschutzgesetze an die EU-Datenschutzrichtlinie sind den Gesetzgebern im Hinblick auf die Kontrolle der Datenverarbeitung und die Transparenz für den Bürger

zwei Alternativen gewiesen worden (Art. 18): Entweder erhalten die Kontrollstellen – das sind die Datenschutzbeauftragten des Bundes und der Länder – *Meldungen über die automatisierten Verfahren,* die einen definierten Mindestinhalt haben (Art. 19) und von jedem einsehbar sind, oder es werden Datenschutzbeauftragte von den verantwortlichen Stellen bestellt, die die Einhaltung der datenschutzrechtlichen Bestimmungen unabhängig überwachen und ein Verfahrensverzeichnis führen, das seinerseits der Öffentlichkeit verfügbar gemacht werden muss. Im letzteren Falle entfällt die Meldung an die Kontrollstelle oder sie wird wesentlich vereinfacht.

Nach dem derzeitig erkennbaren Trend der Novellierung des Bundes- und der Landesdatenschutzgesetze dürfte der zweite Weg gegangen werden. Dies bedeutet, dass für alle öffentlichen und privaten Stellen in Deutschland, die personenbezogene Daten verarbeiten, die Bestellung eines behördlichen oder betrieblichen Datenschutzbeauftragten verbindlich vorgeschrieben wird, sofern die Anzahl der Mitarbeiter, die mit der Verarbeitung der Daten zu tun haben, eine bestimmte Grenze überschritten hat.

Nach der derzeitigen Rechtssituation sind in der privaten Wirtschaft *betriebliche Datenschutzbeauftragte* zu bestellen, wenn mindestens fünf Mitarbeiter mit der automatisierten oder mindestens zwanzig Mitarbeiter bei der nichtautomatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Im öffentlichen Bereich ist die Bestellung behördlicher Datenschutzbeauftragter schon jetzt für Behörden bundesweit vorgeschrieben, die Sozialdaten verarbeiten. Außerdem bestimmen einige Landesdatenschutzgesetze, so auch das Berliner Datenschutzgesetz, dass alle öffentlichen Stellen des Landes *behördliche Datenschutzbeauftragte* zu bestellen haben. Ihre Rechtsstellung wird durch einen Verweis auf die Bestimmungen des Bundesdatenschutzgesetzes zu den betrieblichen Datenschutzbeauftragten bestimmt.

Bei der *Durchsetzung der Bestellung des internen Datenschutzbeauftragten* gibt es deutliche Unterschiede zwischen der privaten Wirtschaft und der öffentlichen Verwaltung. Wird in einem Unternehmen ein betrieblicher Datenschutzbeauftragter nicht oder nicht rechtzeitig bestellt, kann die zuständige Aufsichtsbehörde Bußgelder bis zu fünfzigtausend Deutsche Mark verhängen. Im öffentlichen Bereich kommt es vor, dass selbst große Behörden, die intensiv mit den Daten der Bürger arbeiten, trotz eindeutiger entgegenstehender Rechtslage behördliche Datenschutzbeauftragte für überflüssig erklären und gelassen den Beanstandungen des Landesdatenschutzbeauftragten entgegensehen. Berlin stellt insoweit keine Ausnahme dar.

Mit der Anpassung an die EU-Datenschutzrichtlinie wird sich auch in Berlin die rechtliche Situation der behördlichen Datenschutzbeauftragten insoweit ändern, als sie *zusätzliche Aufgaben* zu erfüllen und zusätzliche Verantwortlichkeiten für den Datenschutz zu übernehmen haben werden. Die bisher schon gesetzlich vorgeschriebenen internen Verzeichnisse und Beschreibungen werden voraussichtlich modifiziert und öffentlich zugänglich gemacht werden. Bei sensiblen Verfahren werden von ihnen Vorabkontrollen durchzuführen sein. Die Unabhängigkeit der behördlichen Datenschutzbeauftragten wird damit ebenso verbreitert werden müssen wie die Bereitstellung personeller und sachlicher Ressourcen.

Um festzustellen, wieweit in den Berliner Behörden die behördlichen Datenschutzbeauftragten auf die bevorstehenden Rechtsänderungen vorbereitet sind, haben wir eine Befragung bei einer Auswahl von behördlichen Datenschutzbeauftragten durchgeführt. Wir wollten feststellen, welchen Umfang ihr Aufgabenspektrum hat, wie stark die Unterstützung in der eigenen Dienststelle ausgeprägt ist und insbesondere auch wie viel Zeit ihnen zur Verfügung steht. Die folgende Zusammenfassung der Ergebnisse stützt sich auf die Befragung von 42 behördlichen Datenschutzbeauftragten in ausgewählten Behörden des Landes Berlin (Senatsverwaltungen und nachgeordnete Behörden, Bezirksämter). In zwei Stellen, die kontaktiert worden waren, waren zu dem Zeitpunkt keine behördlichen Datenschutzbeauftragten bestellt worden.

Bestellung

Die Einbindung der behördlichen Datenschutzbeauftragten in die Behördenstruktur ist uneinheitlich. Es bleibt der Daten verarbeitenden Stelle überlassen, aus welchem Bereich sie ihren Datenschutzbeauftragten rekrutiert. In der Regel kommt er aus einem Arbeitsgebiet, das entweder dem Rechts- bzw. Verwaltungsbereich (Rechtsamt, Organisationsamt, zentrale Verwaltung) oder einem Bereich mit informationstechnischem Zuschnitt (IT-Stelle, EDV-Abteilung, Innenrevision) zuzuordnen ist. Nur in wenigen Fällen ist der Datenschutzbeauftragte in einer Stabsstelle der Behördenleitung angesiedelt. Aber auch aus anderen Bereichen wie z. B. Bürgerberatung, Ausbildung, Jugend oder Bauwesen wurden Datenschutzbeauftragte bestellt.

Es gibt auch Überlegungen, den Posten des behördlichen Datenschutzbeauftragten mit anderen Beauftragtenstellen, z. B. IT-Sicherheitsbeauftragter, Geheimschutzbeauftragter, Korruptionsbeauftragter, Frauenbeauftragte, zu kombinieren, um so der angespannten Haushaltssituation zu begegnen. Hierbei können jedoch *Interessenkonflikte* zwischen den verschiedenen Funktionen auftreten, die die Zuverlässigkeit beeinträchtigen können. Diesen Interessenkonflikten können hinreichend große Behörden natürlich dadurch begegnen, dass sie Datenschutzbeauftragte bestellen, die sich ausschließlich dieser Aufgabe widmen können. Dies ist bisher nur in verschwindend wenigen Behörden geschehen.

Die Einstellung zum Datenschutz drückt sich in manchen Behörden bzw. Ämtern bereits in der Art und Weise aus, wie die Bestellung des Datenschutzbeauftragten im Hause bekannt gemacht wird. Einige Stellen versäumten die *Unterrichtung der Mitarbeiter* und überließen es dem Zufall, ob diese es dem Telefonverzeichnis oder dem Geschäftsverteilungsplan entnehmen, dass es einen behördlichen Datenschutzbeauftragten gibt und um wen es sich handelt. In wenigen Fällen machte sich der Datenschutzbeauftragte selbst mit einem Informationsblatt im Hause bekannt.

Der überwiegende Teil der Daten verarbeitenden Stellen konnte kein *Datenschutzkonzept* oder zumindest eine Sammlung aller den Datenschutz betreffenden Richtlinien, Dienstanweisungen und sonstiger Datenschutzregelungen vorweisen. Die vereinzelt vorhandenen Anweisungen und Richtlinien betrafen im Wesentlichen die Dokumentation von Verfahren und gewisse Sicherheitsregeln für den Umgang mit der Informationstechnik wie zum Umgang mit Passwörtern oder zu Benutzerprofilen. Solche Regelungen sind meistens schon im IT-Konzept enthalten, das in der Regel von der IT-Stelle erstellt wird. Weiter gehende, für den Datenschutz unerlässliche Unterlagen zur Umsetzung der technisch-organisatorischen Anforderungen des Berliner Datenschutzgesetzes gab es nur in wenigen Fällen. Sie betrafen vor allem Regelungen für den Zutritt zu bestimmten Räumen, die Aufbewahrung, den Transport und die Entsorgung von Datenträgern, die Auftragsvergabe nach außen (Outsourcing), das Fernwartungskonzept sowie rein organisatorische Regelungen wie die Schlüsselordnung oder der Katastrophenplan (Vorsorgemaßnahmen für den Datenverlust im Katastrophenfall).

Die gesetzlich mögliche *Bestellung externer Datenschutzbeauftragter* erfolgt in Berliner öffentlichen Stellen nur selten. Wenn dies doch geschieht, dann übernimmt meistens der Datenschutzbeauftragte einer übergeordneten Behörde die Funktion auch für eine nachgeordnete Behörde. Problematisch ist die Bestellung externer Datenschutzbeauftragter auf der Grundlage kurzfristig geltender Werkverträge, insbesondere wenn der Beauftragte von dieser Tätigkeit wirtschaftlich abhängig ist. In diesen Fällen ist sehr zweifelhaft, ob der Datenschutzbeauftragte sein Amt mit der notwendigen Unabhängigkeit wahrnehmen kann, was bedeutet, dass er auch zur Führung kontroverser Auseinandersetzung bereit und fähig sein muss.

Wahrnehmung der Aufgaben

Eine wesentliche Aufgabe des behördlichen Datenschutzbeauftragten ist die *Beratung* zu täglichen Problemen des Datenschutzes, die von Leitungskräften, Mitarbeitern und Auszubildenden, aber auch von Bürgern telefonisch oder schriftlich an ihn herangetragen werden. In der Praxis wird er von Leitungskräften wesentlich weniger konsultiert als von den untergebenen Mitarbeitern. Es ist offensichtlich, dass Führungskräfte dem Datenschutz oft passiv, wenn nicht gar reserviert gegenüberstehen, obwohl sie den Datenschutz im Hause verantwortlich umsetzen müssen, während die Mitarbeiter sich hinsichtlich ihres Verhaltens beim Datenschutzbeauftragten absichern oder sich als Betroffene an ihn wenden.

In einigen Fällen sind die Daten verarbeitenden Stellen dazu übergegangen, die *Stellungnahmen zu unseren Beanstandungen oder zu unserem Jahresbericht* von ihrem behördlichen Datenschutzbeauftragten erarbeiten zu lassen. Es kann jedoch nicht seine Aufgabe sein, datenschutzrechtliche Mängel im eigenen Hause, für die die Behördenleitung die Verantwortung trägt, gegenüber der externen Kontrollinstanz zu rechtfertigen, zumal er auf Grund seiner Fachkunde und seinem am Datenschutz orientierten Interesse dabei meist gegen seine eigene Überzeugung argumentieren müsste. Seine Aufgabe ist es vielmehr, die Verantwortlichen datenschutzrechtlich zu beraten, die fachübergreifenden Stellungnahmen im Hause zu koordinieren, auf die erforderlichen Maßnahmen zu drängen und ihre Durchführung zu kontrollieren.

Das Interesse der Verantwortlichen an Datenschutzbelangen zeigt sich vor allem dort, wo der behördliche Datenschutzbeauftragte aufgefordert wird, die Defizite beim Datenschutz zu ermitteln und zusammenzustellen, um die Voraussetzungen für Verbesserungen zu schaffen, oder wo der Datenschutzbeauftragte mit dem gleichen Ziel regelmäßige Tätigkeitsberichte einbringt. Leider ist ein solches offensives Interesse am Datenschutz in den Berliner Behörden selten vorzufinden, so dass die Tätigkeit der Datenschutzbeauftragten weder die nötige Würdigung und Anerkennung finden noch die notwendige Wirkung erzielen kann. Der Datenschutzbeauftragte hat dann nur eine *Alibifunktion.* Seine Bestellung erfolgt nur als Formalie, nicht jedoch in der Absicht, den Datenschutz sicherzustellen, wie es das Datenschutzgesetz verlangt.

Zur *Durchführung eigener Kontrollen* – z. B. der Beachtung der technisch-organisatorischen Kontrollanforderungen nach § 5 BlnDSG – haben die wenigsten behördlichen Datenschutzbeauftragten Zeit und Gelegenheit. Wenn überhaupt, werden derartige Kontrollen meist nur anlässlich von Beschwerden oder offenkundig gewordener Datenschutzverstöße durchgeführt. Diese unzulängliche Kontrolltätigkeit beruht auf dem geringen *Zeitrahmen,* den die meisten behördlichen Datenschutzbeauftragten für ihre Tätigkeit zur Verfügung haben, sowie auf der häufig für solche Kontrollen unzureichenden *Fachkunde.*

Die *Koordinierungsrunde der bezirklichen Datenschutzbeauftragten,* in der sich seit langem ein Teil der Datenschutzbeauftragten der Bezirksämter unter unserer Beteiligung trifft, hat zur Verbesserung der Prüfaktivitäten die Initiative ergriffen und eine Checkliste erstellt, die eine gezielte Kontrolltätigkeit auf einer relativ pauschalen Ebene ermöglicht. Die Erfahrung zeigt, dass schon die konsequente Verfolgung einiger elementarer und einfach zu überwachender Sicherheitsziele zu erheblichen Verbesserungen des Datenschutzes führen kann.

Der behördliche Datenschutzbeauftragte hat bei der *Einstellung von Personal,* das bei der Verarbeitung personenbezogener Daten tätig sein soll, beratend mitzuwirken. Dies geschieht fast nie, weil die Unterrichtung von solchen Einstellungsvorgängen unterbleibt und das verfügbare Zeitbudget für diese aufwendige Aufgabe nicht ausreicht.

Eine weitere vom Gesetz vorgesehene Aufgabe des behördlichen Datenschutzbeauftragten ist es, die Mitarbeiter durch geeignete *Schulung* mit den Datenschutzregelungen im Allgemeinen und den spezifischen Regelungen des Hauses im Besonderen vertraut zu machen. Einige behördliche Datenschutzbeauftragte erledigen dies in vorbildlicher Art und Weise und übergeben bereits bei der Einstellung von neuen Mitarbeitern Schulungsmaterial oder halten Einführungskurse ab, in denen sie die wichtigsten Datenschutzvorschriften vermitteln. Besonders lobenswert ist es, wenn darüber hinaus gesonderte Schulungen zu bestimmten Schwerpunktthemen abgehalten werden oder aber die Schulungen in regelmäßigen Abständen wieder aufgefrischt werden. Leider gibt es aber auch viele Fälle, in denen man sich mit der Übergabe einfacher Merkblätter begnügt oder gar die Einweisungspflicht gänzlich vernachlässigt.

Die *Führung von internen Datei- und Geräteübersichten* und damit zusammenhängend die Meldung zum Berliner Dateienregister beim Berliner Datenschutzbeauftragten wird meistens sehr stiefmütterlich behandelt. Nur selten werden die Übersichten aktuell und vollständig geführt. Meist sind die Unterlagen veraltet und nur lückenhaft, zum Teil nur schwer zugänglich, weil sie in den Behörden verstreut aufbewahrt werden. Dabei müsste es für die Daten verarbeitende Stelle von größtem Eigeninteresse sein zu wissen, welche Geräte und Programme sie für welche Aufgaben und Verfahren einsetzt und welche Dateien dabei verarbeitet werden. Zu den Geräten mussten die Stellen schon immer – auch ohne direkten Datenschutzbezug – einen Maschinennachweis führen und mit der geplanten Neugestaltung des INVENT-Verfahrens wird die Geräteübersicht ihre Bedeutung erweitern.

Sollte die aufwendige Meldung zum Berliner Dateienregister fortfallen, so wird es den datenverabeitenden Stellen umso mehr auferlegt sein, ihre Datei-, Verfahrens- und Geräteübersichten aktuell und vollständig zu führen. Das Recht des Bürgers, in diese Übersichten Einsicht zu nehmen, bleibt erhalten, wird aber bei den Daten verarbeitenden Stellen selbst zu gewähren sein. Darauf sind sie allerdings bisher weitgehend unvorbereitet.

Persönliche Voraussetzungen

Zuverlässigkeit und Fachkunde sind die vom Gesetz vorgegebenen wichtigsten Voraussetzungen für die Qualifikation zum behördlichen Datenschutzbeauftragten.

Die *Fachkunde* umfasst Kenntnisse des Datenschutzrechts und des Spezialrechts der im Hause vertretenen verschiedenen Fachgebiete, insbesondere des Personalrechts, sowie zum technischen und organisatorischen Datenschutz und zu den eingesetzten automatisierten Datenverarbeitungsverfahren und ihren informationstechnischen Plattformen. Zudem sind didaktische Fähigkeiten erforderlich, damit der behördliche Datenschutzbeauftragte die Mitarbeiter im Rahmen von Schulungsmaßnahmen mit den Datenschutzvorschriften vertraut machen kann.

Wir haben den idealen Datenschutzbeauftragten nirgends vorgefunden. Die meisten Befragten haben jedoch entweder einen juristischen oder informatischen Qualifikationshintergrund. Wenn Fortbildungsmaßnahmen in dem weniger vertrauten Bereich genutzt werden und die Unterstützung von Fachleuten des jeweils anderen Gebietes gesucht wird, kann die erforderliche Fachkunde angemessen erreicht werden.

Der für die Tätigkeit als behördlicher Datenschutzbeauftragter *verfügbare Zeitrahmen* setzt weitere Grenzen für die Umsetzung des Datenschutzes. Lediglich in fünf der besuchten Behörden nehmen die behördlichen Datenschutzbeauftragten ihre Aufgaben als Vollzeitkräfte wahr. Dabei haben alle auch einen Stellvertreter und mitunter auch weitere Mitarbeiter, so dass der Datenschutz hier weitgehend gewährleistet werden kann. In der Regel handelt es sich bei diesen Stellen um große Behörden mit sensiblen Bereichen, in denen von der Sache her schon ein erhöhtes Augenmerk auf die datenschutzgerechte Datenverarbeitung gelegt werden muss. Dieses zunächst positive Bild relativiert sich jedoch, wenn man bedenkt, dass nicht ein repräsentativer Querschnitt der zur Bestellung behördlicher Datenschutzbeauftragter verpflichteter Behörden besucht wurde. Tatsächlich standen größere Behörden im Vordergrund der Betrachtung.

Selbst dort können bei den meisten Stellen die behördlichen Datenschutzbeauftragten nur ca. 10 % und weniger von ihrer Arbeitszeit für den Datenschutz aufwenden. Mit diesem Zeitumfang können die Datenschutzbeauftragten nicht einmal die unmittelbaren gesetzlichen Pflichten erfüllen. Es wird ihnen überlassen, mit diesem Defizit klar zu kommen. In einigen Fällen wird ihnen seitens der Behördenleitung sogar zu verstehen gegeben, dass das eigentliche Aufgabengebiet zu jeder Zeit Vorrang hat vor Datenschutzbelangen. Damit verletzen die Verantwortlichen nicht nur ihre gesetzlich verankerte Unterstützungspflicht für den Datenschutzbeauftragten, sondern auch ihre Fürsorgepflicht.

In einem Fall weigert sich ein Bezirksamt seit langem beharrlich, einen behördlichen Datenschutzbeauftragten zu bestellen. Die Aufgaben nimmt der *Direktor beim Bezirksamt* wahr, was wegen seiner Verantwortung für das Personalwesen und für viele andere Anwendungsfelder personenbezogener Datenverarbeitung den Kriterien für einen

zuverlässigen Datenschutzbeauftragten in extremer Weise widerspricht. Es ist offenkundig, dass hier der „lästige Datenschutz“ an richtiger Stelle gleich im Keim erstickt werden soll.

In einer Senatsverwaltung wurde zwar ein behördlicher Datenschutzbeauftragter formell verpflichtet, da aber nach seiner Auffassung personenbezogene Daten kaum verarbeitet würden, hielt er weder von der eigenen Fortbildung etwas noch von der Bereithaltung eines Dateien- und Geräteverzeichnisses. Auch wenn diese Senatsverwaltung ein Ressort darstellt, in dem die Verarbeitung personenbezogener Daten nicht den Schwerpunkt der Aufgabenerfüllung darstellt, ist die Bestellung eines *Pseudo-Datenschutzbeauftragten* unangemessen.

Dennoch ist das Engagement der meisten befragten Datenschutzbeauftragten zu loben. Trotz unzureichenden Zeitbudgets und geringer sachlicher Ausstattung bemühen sie sich darum, die Behördenleitungen in ihrer Verantwortung für den Datenschutz zu entlasten. Sie geben hilfreiche Anregungen zur Verbesserung des Datenschutzes in ihren Zuständigkeitsbereichen und nützliche Denkanstöße zur Zusammenarbeit untereinander und mit dem Berliner Datenschutzbeauftragten.

Unterstützung

Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere Hilfspersonal, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Bei dieser Prämisse stimmt nachdenklich, dass viele Befragte Anlass zu der Feststellung sahen, dass die *Leitungskräfte* nur wenig Akzeptanz für den Datenschutz aufbringen. Datenschutzbelange, die gerade zwingend erforderlich sind und wenig kosten, werden zwar meistens unterstützt, doch sobald eine Maßnahme mit zusätzlichen Kosten oder hohem organisatorischem Aufwand verbunden ist, wird ihnen nur noch eine geringe Priorität eingeräumt. Das machte sich besonders bei der Genehmigung von Schulungs- und Fortbildungsveranstaltungen oder aber der Entwicklung und Ausarbeitung eines übergreifenden Datenschutzkonzepts bemerkbar. Leere Haushaltskassen rechtfertigen jedoch auch beim Datenschutz nicht, der Pflicht zum gesetzmäßigen Handeln auszuweichen.

In vielen großen öffentlichen Stellen, zum Beispiel in den Bezirksämtern, vielen Senatsverwaltungen, Hochschulen, Krankenhäusern oder großen nachgeordneten Behörden sind die datenschutzrechtlichen und technisch-organisatorischen Fragestellungen so vielfältig und komplex, dass von dem behördlichen Datenschutzbeauftragten nicht erwartet werden kann, dass er zu allen Fragestellungen gleichermaßen die notwendige Fachkunde aufbringen kann. Es ist daher wichtig, dass ihm in solchen Stellen Kollegen bzw. *Spezialisten aus einzelnen Fachgebieten* hilfreich zur Seite stehen. Darüber hinaus sind große Behörden vielfach

auch räumlich verteilt, so dass manche Standorte nur selten Kontakt mit dem behördlichen Datenschutzbeauftragten haben. In diesen Fällen sollten Kontaktleute benannt werden, die dem behördlichen Datenschutzbeauftragten zuarbeiten, eventuell sogar dessen Aufgaben vor Ort wahrnehmen. Eine solche Datenschutzinfrastruktur ist in einigen öffentlichen Stellen durchaus vorhanden, der Erfahrungsaustausch zwischen dem Datenschutzbeauftragten und den Kontaktleuten lässt jedoch meist zu wünschen übrig.

Die Akzeptanz der *Belegschaft* für den Datenschutz ist in vielen Stellen durchaus vorhanden, doch könnte sie noch stärker ausgeprägt sein. Immer wieder gibt es Situationen, in denen der Datenschutz als Behinderung beim täglichen Umgang mit personenbezogenen Daten angesehen wird. Mitunter dient er auch als Vorwand, um ungelegene Tätigkeiten und Mehrarbeit zu vermeiden. Erst wenn jemand selbst Betroffener oder Geschädigter ist, wird das Interesse am Datenschutz geweckt und die notwendigen Schutzmaßnahmen auch verstanden und akzeptiert.

Die *Schulung* der behördlichen Datenschutzbeauftragten lässt allgemein zu wünschen übrig. Weil nur wenig Zeit für die Datenschutztätigkeit zur Verfügung steht, fehlt sie erst recht für die eigene stetige Fortbildung auf diesem Gebiet. Diese ist jedoch immens wichtig, denn die rechtliche und technische Entwicklung schreitet schnell voran und stellt an den behördlichen Datenschutzbeauftragten hohe Anforderungen an die Aktualisierung des Wissens. Die Befragung ergab, dass der überwiegende Teil keine oder nur sehr wenig Zeit für Fortbildungsmaßnahmen hat. Die Zeit reicht höchstens für die Lektüre von Datenschutzschriften oder -kommentaren, doch für längere Dienstunterbrechungen, z. B. für Fortbildungskurse, bleibt kaum Freiraum übrig.

In Berlin sind die Schulungsmöglichkeiten leider begrenzt. Es gibt keine offizielle Ausbildungsstätte für behördliche Datenschutzbeauftragte, so dass dem Wunsch vieler Datenschutzbeauftragter nach fundierter und einheitlicher Grundausbildung leider nicht entsprochen werden kann. Die überregionalen Bildungsinstitute sind nur im Zusammenhang mit einer Dienstreise zu erreichen, was mit zusätzlichen Kosten verbunden und daher für viele nicht tragbar ist. Der Berliner Datenschutzbeauftragte, der personell nicht entsprechend ausgestattet ist, kann in Berlin den offenkundigen Schulungsbedarf nicht abdecken. Einige unserer Mitarbeiter beteiligen sich als Dozenten an dem einschlägigen Lehrangebot zum Datenschutz und zur informationstechnischen Sicherheit der Verwaltungsakademie. Jedoch zeigt sich auch hier, dass sich das Interesse an Fortbildungsmaßnahmen für behördliche Datenschutzbeauftragte in Grenzen hält und auf relativ wenige besonders interessierte Personen beschränkt, die zum Beispiel in Auffrischungsworkshops ihr Wissen aktualisieren.

4. Aus den Arbeitsgebieten

4.1 Sicherheit

4.1.1 Polizei

Nachdem zum Übereinkommen vom 26. Juli 1995 aufgrund von Art. K 3 des Vertrages über die Europäische Union über die Errichtung eines Europäischen Polizeiamtes *(Europol-Übereinkommen)*[88] alle Mitgliedstaaten der Europäischen Union die Ratifizierungsurkunde hinterlegt haben, ist das Übereinkommen zum 1. Oktober 1998 in Kraft getreten. Der Bundesrat hat nach Art. 2 § 6 Abs. 2 Europol-Gesetz den Landesbeauftragten für den Datenschutz Sachsen-Anhalt als Landesvertreter für die gemeinsame Kontrollinstanz benannt.

Mit dem Ersten Gesetz zur *Änderung des Bundesgrenzschutzgesetzes*[89] sind die Befugnisse des Bundesgrenzschutzes erweitert worden, der künftig auf Bahnhöfen, Flughäfen und in Zügen im Rahmen der so genannten *„Schleierfahndung"* ohne konkreten Verdacht auf eine Straftat Ausweise kontrollieren darf, um eine illegale Einreise zu verhindern (§ 22 BGSG). Weiter gehende Maßnahmen – wie die Durchsuchung des Gepäckes – sind nur bei konkretem Verdacht zulässig. Diese Neuregelung ist zunächst auf fünf Jahre befristet. Der Grundsatz, dass Bürger, die sich nichts haben zuschulden kommen lassen, das Recht haben, vom Staat in Ruhe gelassen zu werden, wird damit ein weiteres Mal eingeschränkt. Ähnliche Vorstellungen wurden in Berlin entwickelt.

Neue Verwaltungsvorschriften – Datenschutz bleibt außen vor

Das Bundeskriminalamt (BKA) hat für jede zur Erfüllung der Aufgaben geführte Datei mit personenbezogenen Daten in einer Errichtungsanordnung Festlegungen über Rechtsgrundlage und Zweck der Datei, betroffenen Personenkreis und Art der zu speichernden Daten, Prüffristen, Löschungsdauer und Protokollierungen zu treffen. Der Bundesbeauftragte für den Datenschutz ist vor Erlass der Errichtungsanordnung anzuhören. Bei Daten des Polizeilichen Informationssystems bedarf die Anordnung auch der Zustimmung der zuständigen Innenministerien bzw. Senatsinnenverwaltungen der Länder (§ 34 Bundeskriminalamtsgesetz (BKAG)).

Die Senatsverwaltung für Inneres beteiligt uns zu unserem Befremden und dem Unverständnis in anderen Ländern grundsätzlich nicht in diesen Zustimmungsverfahren. Sie vertritt dazu die Auffassung, dass es sich hierbei um Vorgänge handelt, die in die datenschutzrechtliche Verantwortung des BKA fallen und von dem Bundesbeauftragten für den Datenschutz zu überprüfen sind. Demzufolge erhalten wir weder die Entwürfe noch später die in Kraft gesetzten *Errichtungsanordnungen*.

[88] BGBl. II, 2930
[89] vgl. 1.1

Das begründet die Senatsverwaltung für Inneres damit, dass sich die Kontrollbefugnis der Landesdatenschutzbeauftragten auf die von den Ländern eingegebenen Datensätze beschränke. Deshalb liege es auch nicht in deren Aufgabenbereich, zu generell-abstrakten Regelungen Stellung zu nehmen. Im Übrigen würde sich die gesetzliche Unterstützungspflicht auch nicht darauf erstrecken, den Landesbeauftragten mit Entwürfen des BKA zu versorgen oder jede Äußerung gegenüber dem Bundesministerium des Innern zu datenschutzrechtlichen Fragen im Zusammenhang mit Dateien der Polizeilichen Informationssysteme mit uns abzustimmen.

Ungeachtet der Form des Umganges verkennt die Senatsverwaltung für Inneres dabei, dass wir unsere gesetzlichen Aufgaben nur dann erfüllen können, wenn wir die Errichtungsanordnungen kennen. Nur so können wir prüfen, ob Datenübermittlungen an das BKA nach Landesrecht überhaupt zulässig sind. Darüber hinaus gehört es nach § 24 Abs. 1 BlnDSG zu unseren Aufgaben, die einzelnen Mitglieder des Senates zu beraten.

Wie nötig das ist, hat sich bei der Errichtung einer Zentralen Datei für Verdachtsanzeigen im Zusammenhang mit der Bekämpfung der organisierten Kriminalität *nach dem Geldwäschegesetz* gezeigt. Die Errichtung dieser Verbunddatei halten wir für unzulässig, weil dafür – wie das BKA selbst einräumt – keine Rechtsgrundlage vorhanden ist. Hinzu kommt, dass die Registrierung personenbezogener Daten im Zusammenhang mit Ermittlungsverfahren der Staatsanwaltschaften der Länder in deren Zuständigkeiten fällt. Es handelt sich nicht um die Angelegenheiten des BKA. Hier wäre vielmehr zu prüfen, ob eine Speicherung in dem länderübergreifenden Staatsanwaltschaftlichen Verfahrensregister nach §§ 474 ff. StPO in Betracht kommt. Ungeachtet dessen wäre es Mindestvoraussetzung, dass in die Datei nur die Daten aus den Verdachtsanzeigen eingestellt werden, bei denen ein Ermittlungsverfahren eingeleitet wurde. Verdachtsanzeigen, die kein Ermittlungsverfahren auslösen, erfüllen in keinem Fall die Voraussetzungen nach § 8 Abs. 2 BKAG.

Auch die Errichtungsanordnung für die *DNA-Analysedatei*[90] ist äußerst problematisch. Die Speicherung der DNA-Analysen, die auf der Basis von „Einwilligungen" vor In-Kraft-Treten der neuen §§ 81 a und f StPO erhoben wurden, ist unzulässig. Nach § 3 Satz 1 DNA-Identitätsfeststellungsgesetz dürfen – abgesehen von den Fällen des § 81 g StPO – nur die Identifizierungsmuster von Verurteilten beim BKA gespeichert werden. Speicherungen aufgrund von Einwilligungen kommen ohnehin nicht in Betracht, weil die Wirksamkeit eine umfassende Aufklärung über den Zweck der Speicherung und die vorgesehenen Übermittlungen voraussetzt. Es kann nicht angenommen werden, dass die Betroffenen die schwer zu durchschauenden Verarbeitungsformen der Errich-

[90] vgl. zum DNA-Identitätsfeststellungsgesetz 4.3.1

tungsanordnung bis hin zu Übermittlungen in das Ausland nachvollziehen können. Sie müssten in allen Details informiert werden, wogegen bereits die Klassifizierung als Verschlusssache spricht. Darüber hinaus sprechen die Umstände, unter denen DNA-Untersuchungen relevant werden, gegen die Annahme von Freiwilligkeit. Beschuldigte in Strafermittlungsverfahren und Inhaftierte werden nach allgemeiner Lebenserfahrung nur deshalb einwilligen, um unmittelbare Vorteile – beispielsweise Haftverschonung oder vorzeitige Entlassung – zu erlangen.

Für eine Personenabfrage gibt es selbst nach Auffassung des BKA kein fachliches Erfordernis, da Zweck der Datei der Vergleich von DNA-Mustern und nicht der zielgerichtete Abruf von Personendaten ist. Auch die Dateirecherche in der beabsichtigen Form zu statistischen Zwecken ist mit § 3 DNA-Identitätsfeststellungsgesetz nicht vereinbar.

Die Senatsverwaltung für Inneres hat uns auch über das *Zustandekommen des Abkommens zwischen Deutschland und Polen über die Zusammenarbeit der Polizei und Grenzschutzbehörden in den Grenzgebieten* nicht informiert. Das Dokument haben wir vielmehr von dritter Seite erhalten. Es ist mit dem Berliner Landesrecht nicht in Einklang zu bringen. So weist die übermittelnde Behörde bei der Datenweitergabe auf die nach innerstaatlichem Recht geltenden Löschungsfristen hin. Da das ASOG bei Tatverdächtigen keine Löschungs-, sondern nur Prüffristen kennt, hätte zumindest in einer Protokollnotiz sichergestellt werden müssen, dass Prüffristen den Löschungsfristen gleichzusetzen sind. Dem ist die Senatsverwaltung für Inneres nicht nachgekommen. Auf unseren Hinweis, dass die Berliner Polizei verpflichtet ist, die polnischen Behörden wenigstens auf die Prüffristen hinzuweisen, wurde überhaupt nicht reagiert.

Unserer Bitte um Übersendung eines Ergänzungsabkommens hat die Senatsverwaltung für Inneres zunächst nicht entsprochen. Vielmehr hat sie uns gebeten, zur Kenntnis zu nehmen, dass dieser Entwurf keine datenschutzrechtlichen Vorschriften enthalte. Demgegenüber haben wir darauf hingewiesen, dass wir uns darüber gern selbst ein Bild machen würden. Umso überraschter waren wir dann bei der Durchsicht der uns am Ende doch übersandten Unterlagen: Der Entwurf enthielt an verschiedenen Stellen Regelungen zu Ermittlungen, Beantwortung von Ersuchen, Datenaustausch oder Beteiligung in gemischten Arbeitsgruppen. Offensichtlich ist der Innenverwaltung nicht klar, was informationelle Selbstbestimmung bedeutet.

Die von uns seit Jahren geforderte Überarbeitung der *Geschäftsanweisung über erkennungsdienstliche Maßnahmen* ist erfolgt und am 2. Februar 1998 in Kraft gesetzt worden. Wir wurden trotz eines Beschlusses des Unterausschusses Datenschutz des Abgeordnetenhauses nicht gehört – der Polizeipräsident hatte die Geschäftsanweisung am Tage vor der Beratung unterschrieben, ohne dass dies in der Sitzung bekannt gegeben wurde.

Im Unterausschuss bestand Einvernehmen darüber, dass die Zulässigkeit von ed-Maßnahmen bei Bagatelldelikten in der Geschäftsanweisung geregelt werden soll. Das ist nicht geschehen. Weiterhin sind – entgegen früheren Empfehlungen – keine besonderen Regelungen über die ed-Behandlung bei Identitätsfeststellungen an „gefährlichen Orten“ enthalten (§ 21 ASOG). Die von der Polizei geäußerte Auffassung, dass das nicht erforderlich sei, weil eine ed-Behandlung nur das letzte Mittel zur Identifizierung einzelner Personen ist, wenn diese durch eine Kontrolle mitgeführter Identitätspapiere nicht möglich ist, geht an dem Problem vorbei. Festzulegen ist, unter welchen Voraussetzungen ed-Behandlungen zur „vorbeugenden Straftatenbekämpfung“ zulässig sind, die auch erfolgen können, wenn der Betroffene sich ausweisen kann[91]. Weiterhin sollen ed-Maßnahmen bei Unverdächtigen nach deren Einwilligung möglich sein. Ungeachtet der Problematik der „Freiwilligkeit“ bei Einwilligungen gegenüber Sicherheitsbehörden ist hier der Sinn und Zweck nicht klar.

Auch die *Geschäftsanweisung über die Führung kriminalpolizeilicher Personenakten* war bereits vor der Übersendung an uns schlussgezeichnet, wenn auch noch nicht in Kraft gesetzt. Wir haben bemängelt, dass zur Kriminalakte auch Unterlagen über die Versagung oder Entziehung von Führerscheinen, über die Erteilung oder Versagung von Waffen-, Jagd- und Giftscheinen sowie Konzessionen und Berufsverbote zu nehmen sind. Der Zusammenhang zwischen ordnungsrechtlichem Verwaltungsverfahren und vorbeugender Straftatenbekämpfung ist nicht erkennbar. Die Erforderlichkeit der Speicherung von Gutachten und Stellungnahmen von Ärzten und der Sozialen Gerichtshilfe erscheint zweifelhaft, zumal die Geschäftsanweisung den Umstand unberücksichtigt lässt, dass es sich – vor allem bei Auskünften von Ärzten – um hochsensible Daten handelt, die der Schweigepflicht unterliegen. Ebenso wenig ist für Erkenntnisse über geistige oder körperliche Gebrechen, Pflegschaften, Unterbringung in Heil- und Pflegeanstalten, Entmündigungen und Fürsorgeerziehung der Zusammenhang zur vorbeugenden Straftatenbekämpfung ersichtlich.

Die Speicherung von Vermissten-Vorgängen und Unterlagen über versuchte Selbsttötungen in Kriminalakten halten wir für unzulässig. Zwar zählt die Bearbeitung von Vermissten-Anzeigen und Suizidversuchen zu den Aufgaben der Polizei. Bei diesen Vorgängen handelt es sich – mangels Straftatbestand – jedoch nicht um Ermittlungsverfahren. Die in diesem Zusammenhang anfallenden Daten dürfen allenfalls zur Dokumentation oder Vorgangsverwaltung – außerhalb der Kriminalakte –, nicht aber zur vorbeugenden Straftatenbekämpfung gespeichert werden.

---

91 JB 1997, 3.1

Nochmals: Erbe der DDR

Wir hatten in der Vergangenheit über die von der Polizei übernommenen Datenbestände der *Volkspolizei* berichtet[92]. In einem Schlussbericht hat uns der Polizeipräsident in Berlin mitgeteilt, dass die Datenbestände weitgehend vernichtet und das Archiv des Präsidiums aufgelöst wurden. Von dem verbliebenen Rest

- hat das Landesarchiv ca. 400 Meter Archivgut übernommen,
- sind abschließend aufgezählte Unterlagen der Zentralen Ermittlungsstelle für Regierungs- und Vereinigungskriminalität (ZERV) für die Zwecke der Strafverfolgung übergeben worden und
- sind die im Archiv (mit Ausnahme der bei der ZERV befindlichen) vorhandenen Rapporte und alle Chroniken der Polizeihistorischen Sammlung zur Verfügung gestellt worden.

Beim Landeskriminalamt bleiben lediglich ein Arbeits- und ein Archiv-Indexordner.

Die *Vernichtung* der Datenbestände erfolgte fast ein Jahr später, als zwischen der Senatsverwaltung für Inneres, der Polizei und uns vereinbart worden war. Aus den übernommenen Karteien und Dateien sind die nach dem neuen Recht zulässigen Daten in den Bestand in der Kriminalpolizeilichen Datensammlung überführt oder anderweitig weitergeführt worden. Nicht mehr erforderliche Daten sind bis zum In-Kraft-Treten des Berliner Datenschutzgesetzes vom 17. Dezember 1990 bei der Durchsicht gelöscht worden. Alle Daten, die nicht in den Bestand der Kriminalpolizeilichen Datensammlungen übernommen bzw. dem Landesarchiv übergeben, aber gleichwohl weiter aufbewahrt wurden, sollten zum 31. Dezember 1996 vollständig gelöscht werden. Bis dahin durften diese Daten zu Rehabilitationszwecken genutzt werden.

Dennoch wurde den Mitarbeitern der ZERV Einsicht in die gesperrten Unterlagen gewährt. Darüber hinaus wurden auch nach dem 31. Dezember 1996 einzelne Teilbereiche des Archives (Rapporte, Tagebücher der Volkspolizeiinspektionen, eingestellte Ermittlungsverfahren) weiterhin zur polizeilichen Aufgabenerfüllung genutzt. Das ist unzulässig, weil die Sperrung der Daten – also die Nutzungsbeschränkung für bereits durchgesehene und für polizeiliche Zwecke nicht mehr erforderliche Unterlagen ausschließlich für Rehabilitationszwecke – nicht beachtet worden ist.

Adressermittlung durch den Kontaktbereichsbeamten

Eine Petentin beschwerte sich darüber, dass ein Kontaktbereichsbeamter durch Nachfragen bei ihrem Untermieter, ihrem Vermieter, in der Hausgemeinschaft und in der Nachbarschaft ihren Aufenthaltsort ermitteln wollte.

[92] vgl. JB 1991, 2.2

Die Post hatte einen an einen ehemaligen Untermieter der Petentin adressierten Brief mit dem Hinweis „Unbekannt verzogen“ an ein Gericht zurückgesandt. Das Gericht hat daraufhin den Kontaktbereichsdienst um eine *Hausermittlung* ersucht. Im Melderegister war noch die Anschrift bei der Petentin gespeichert. Bei der Ermittlung vor Ort wurde der jetzige Untermieter der Petentin angetroffen, der allerdings keine Angaben machen konnte. Ihm wurde ein Auszugsmitteilungsformular mit der Bitte überreicht, dieses der Hauptmieterin (der Petentin) zum Ausfüllen zu übergeben, wenn der frühere Untermieter dort nicht mehr wohnt. Der Versuch, die Auszugsmitteilung wieder abzuholen, scheiterte deshalb, weil der Kontaktbereichsbeamte bei mehreren Besuchen zu den unterschiedlichsten Tageszeiten weder die Petentin noch den früheren Untermieter angetroffen hat. Deshalb wurden die Vermieterin der Petentin und eine Hausbewohnerin befragt, ob ihnen bekannt sei, wann die Petentin in ihrer Wohnung erreichbar wäre. Die Polizei hält diese Befragungen für zulässig.

Nach § 25 MeldeG darf die Meldebehörde anderen öffentlichen Stellen Daten aus dem Melderegister übermitteln. Sofern ein Empfänger von Meldedaten feststellt, dass die übermittelten Daten offensichtlich nicht (mehr) richtig sind, hat er das der Meldebehörde mitzuteilen. In diesem Zusammenhang kann er um Notierung seiner Anfrage ersuchen, die dann für die Dauer von zwei Jahren nach dem Ende des Jahres der Anfrage gespeichert werden darf.

Das *Landeseinwohneramt* hat die in Berlin wohnhaften Einwohner und deren Wohnungen zu registrieren, um die für die rechtmäßige Erfüllung der Aufgaben öffentlicher Stellen erforderlichen Grunddaten feststellen und nachweisen zu können. Weiterhin hat es das Melderegister von Amts wegen fortzuschreiben, wenn sich gespeicherte Daten geändert haben oder neue Daten zu speichern sind. Wenn die Meldeverhältnisse unklar sind, hat die Meldebehörde sie zu klären. Sofern das Melderegister fortzuschreiben ist, erhält die anfragende Stelle im Fall eines gespeicherten Notierungsersuchens auch die neue Wohnanschrift mitgeteilt. Die Auskunft über den Aufenthalt von Bürgern zu erteilen ist Aufgabe der Meldebehörde und nicht der Polizei. Die Amtshilfevorschriften (§§ 4, 5 VwVfG) können nicht herangezogen werden, da sie lediglich die Verpflichtung zur Amtshilfe regeln. Sie verweisen – was die Zulässigkeit der Hilfeleistung betrifft – auf außerhalb des Verfahrensgesetzes bestehende Rechtsvorschriften und -grundsätze (§ 5 Abs. 2 VwVfG).

Bestehen berechtigte Zweifel an der Richtigkeit der gespeicherten Anschrift eines Meldepflichtigen, muss die Meldebehörde zur Klärung den Betroffenen selbst befragen. Dieser hat mitzuteilen, ob er noch immer dort gemeldet ist. Führt das nicht zu dem gewünschten Erfolg, kann im Rahmen der Nebenmeldepflicht der Vermieter befragt werden. Erst wenn auch diese Befragung erfolglos bleibt, sind weitere Ermittlun-

gen, Befragungen und Datenerhebungen im Rahmen des ASOG zulässig. Die Polizei wird im Zusammenhang mit Adressermittlungen für die Meldebehörde tätig, weil diese keinen eigenen Ermittlungsdienst hat. Sie hat keine über die Befugnisse der Meldebehörde hinausgehenden Rechte. Das Ergebnis der Befragung ist dann auch der Meldebehörde zwecks Entscheidung über die Fortschreibung des Melderegisters zu übersenden. Im Ergebnis bedeutet das für den zugrunde liegenden Sachverhalt, dass gegen den Versuch, zunächst den Meldepflichtigen und danach die Petentin als Vermieterin zu befragen, keine Bedenken bestehen.

Die Befragungen hinsichtlich der Petentin sind damit allerdings nicht abgedeckt. Es geht hier um die Klärung der Meldeverhältnisse des Untermieters und nicht um die der Hauptmieterin (der Petentin). Bekanntermaßen gibt es vielfältige Gründe für eine Abwesenheit von der Wohnung, beispielsweise eine Reise, mit der Folge, dass die Versuche des Kontaktbereichsbeamten – auch zu unterschiedlichen Zeiten – erfolglos bleiben müssen. Die Person, die zum – unbekannten – Aufenthalt eines – gesuchten – Dritten etwas erklären soll, wird selbst Gegenstand von Ermittlungen, ohne dass dafür ein Auftrag oder Ersuchen vorliegt.

Sippenhaft für die bei der Polizei eingesetzten Dolmetscher?

In einem Fernschreiben an alle Schutz- und Kriminalpolizeidienststellen sowie die Senatsverwaltungen für Inneres und Justiz hat das Landeskriminalamt davor gewarnt, die Tochter eines Beschuldigten als Dolmetscherin einzusetzen.

Dabei wurden nicht nur die personenbezogenen Daten des Beschuldigten – also des Vaters – übermittelt, sondern die Empfänger vor Beschäftigung der Tochter gewarnt. Die Warnung beschränkte sich nicht nur auf den Einsatz in dem gegen den Vater geführten Ermittlungsverfahren, sondern zielte darauf ab, auf die Dienste der Tochter überhaupt nicht mehr zurückzugreifen.

Diese Datenübermittlung war nicht gerechtfertigt, da die Tochter nicht für Taten des Vaters zur Verantwortung gezogen werden kann. Ungeachtet dessen war bei einer Warnung vor dem Einsatz eines Dolmetschers die Übermittlung von personenbezogenen Daten des Beschuldigten nicht erforderlich. Sofern ein Dolmetscher für den Einsatz für die Polizei ungeeignet ist oder Unzulänglichkeiten und Unregelmäßigkeiten im Zusammenhang mit der Dolmetschertätigkeit bekannt werden, sind besondere Dienststellen des Landeskriminalamtes zu informieren. Sofern nach der Prüfung gesondert noch andere Dienststellen informiert werden müssen, erfolgt das Fernschreiben mit dem Zusatz „VS-NfD“ („Verschlusssache – Nur für den Dienstgebrauch“). Die Polizei hat sich für den übereifrigen Beamten entschuldigt.

Wie bei der Polizei der Verkäufer seines Autos zum Dieb wurde

Ein Berliner hat 1992 sein Auto an einen Händler verkauft und bei der Zulassungsstelle ordnungsgemäß abgemeldet. Der Händler hat seinerseits den Wagen sofort weiterveräußert. Noch im gleichen Jahr hat der Petent eine Vorladung der Polizei zu einer Anhörung in einer Strafsache erhalten. Dabei wurde er noch für den Halter des verkauften – inzwischen gestohlenen – Autos gehalten. Der Petent konnte die Zusammenhänge schnell erklären. Die Polizei hat sich bei ihm entschuldigt. Allerdings fiel er 1998 aus allen Wolken, als ihm im Rahmen der Zuverlässigkeitsüberprüfung für eine waffenrechtliche Erlaubnis vorgehalten wurde, dass er strafrechtlich aufgefallen sei.

Die Staatsanwaltschaft hat uns mitgeteilt, dass sich zum Zeitpunkt des Diebstahles keine Kennzeichen an dem Fahrzeug befanden. Als das gestohlene Fahrzeug aufgrund eines anonymen Hinweises aufgefunden wurde, waren die Kennzeichen eines typengleichen anderen Fahrzeuges befestigt, das in der gleichen Nacht ebenfalls entwendet wurde. Deshalb hatte die Polizei auch Ermittlungen wegen des Vorwurfes des *Kennzeichen-Missbrauches* (§ 22 Straßenverkehrsgesetz [StVG]) aufgenommen. Dabei kam es zu schwer wiegenden Fehlern in der Bearbeitung.

Obwohl der anonyme Hinweisgeber die Polizei ausdrücklich darauf hingewiesen hatte, dass der Pkw gestohlen war, erfolgte nach der Feststellung der Fahrzeugidentifizierungsnummer keinerlei Abfrage, ob nach dem sichergestellten Fahrzeug eine Fahndung bestand. Deshalb konnten weder die Eigentümerin des Fahrzeuges von dem Auffinden unterrichtet noch die nach wie vor bestehende Fahndung nach dem Fahrzeug gelöscht werden. Stattdessen zog die Polizei Erkundigungen nach dem letzten Halter des Wagens ein. Da der Autohändler das Fahrzeug noch nicht auf sich zugelassen hatte, wurde ihr daraufhin der Petent als letzter Halter mitgeteilt.

Obwohl aus der bloßen Haltereigenschaft nicht der Schluss gezogen werden kann, dass eine mit dem Fahrzeug verübte Straftat auch vom Halter begangen wurde, ist der Petent als Beschuldigter zur Vernehmung wegen des Vorwurfes des Kennzeichen-Missbrauches vorgeladen und später *im ISVB* als Beschuldigter mit dem Delikt „Besonders schwerer Diebstahl von Pkw“ eingegeben worden. Erst nachdem der Petent in der Vernehmung die Sachlage erklären konnte, stellte die Polizei die bestehende Fahndung nach dem Fahrzeug fest und löschte sie.

Bei der Staatsanwaltschaft wurde das Verfahren wegen Pkw-Diebstahls und Kennzeichen-Missbrauchs als Unbekannt-Sache eingetragen und ohne Benachrichtigung des Petenten eingestellt. Nach Abschluss der Ermittlungen im Jahr 1992 sind die im Zusammenhang mit dem Ermittlungsvorgang „Verdacht des besonders schweren Diebstahles von Pkw“ gespeicherten Daten bei der Polizei nicht gelöscht worden. Das

verstößt gegen § 48 Abs. 2 ASOG, wonach in Dateien gespeicherte personenbezogene Daten zu löschen und die dazugehörigen Unterlagen zu vernichten sind, wenn ihre Speicherung unzulässig war. Da der Petent wegen des Verdachtes des Kennzeichen-Missbrauches vernommen wurde, war zudem die Speicherung des Tatverdachtes „Besonders schwerer Diebstahl von Pkw“ inhaltlich falsch.

Einen weiteren Mangel stellt die offenbar unterbliebene Überprüfung der Datenspeicherung vor der Übermittlung des Tatverdachtes an die über die waffenrechtliche Erlaubnis entscheidende Behörde dar. Nach § 48 Abs. 2 Satz 1 ASOG ist anlässlich einer Einzelfallbearbeitung – hier der Entscheidung über das Ermittlungsersuchen – zu prüfen, ob die Daten für die Aufgabenerfüllung noch erforderlich sind. Wenn dies erfolgt wäre, hätte die Datenübermittlung unterbleiben und die Löschung der Daten erfolgen müssen. Der Petent war darüber hinaus in anderem Zusammenhang mehr als sechs Jahre als „Geschädigter“ in einer Datei gespeichert. Hier wurde nicht einmal die fünfjährige Speicherungsfrist der Polizei eingehalten[93].

4.1.2 Verfassungsschutz

Sicherheitsüberprüfungen

Das Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Berlin (Berliner Sicherheitsüberprüfungsgesetz [BSÜG]) ist am 12. März 1998 in Kraft getreten[94]. Die hierzu am 11. April 1998 erlassene Allgemeine Verwaltungsvorschrift der Senatsverwaltung für Inneres zur Ausführung des BSÜG (AV BSÜG) enthält Konkretisierungen und Erläuterungen der gesetzlichen Regelungen und die bei Sicherheitsüberprüfungen zu verwendenden Hinweisblätter und Formulare.

Die Ausführungsvorschrift war auch Gegenstand von Beratungen im Unterausschuss „Datenschutz“ des Abgeordnetenhauses. Den Empfehlungen wurde zum Teil gefolgt:

Klargestellt wurde, dass dem Betroffenen, dem einbezogenen Ehegatten/Lebenspartner und Referenzpersonen *Einsicht in die Sicherheits- und die Sicherheitsüberprüfungsakte* zu gewähren ist und dass sie Anspruch auf Auskunft über die in Dateien und Akten über sie gespeicherten Daten haben. Ein besonderes Formular für die Einwilligungserklärung des Ehegatten/Lebenspartners zur längeren Aufbewahrung der Sicherheitsakte ist in der Ausführungsvorschrift vorgesehen und soll erstellt werden. Bei der Polizei wird nur nach anhängigen Ermittlungsverfahren gefragt. Die ursprünglich vorgesehene Auskunft über sämtliche bei der Polizei gespeicherten Verfahren – auch wenn eine Einstellung oder ein Freispruch erfolgte – ist entfallen.

93 vgl. 3.1
94 BSÜG vom 2. März 1998, GVBl. S. 26, vgl. auch JB 1997, 4.1.2

Entfallen ist auch der Hinweis, dass Zweifel an der Zuverlässigkeit entstehen können, wenn der Geheimschutzbeauftragte nicht darüber unterrichtet wird, dass eine Ehe oder eheähnliche Gemeinschaft während oder nach der Sicherheitsüberprüfung eingegangen wurde.

Nachgekommen wurde unserer Empfehlung, die Betroffenen auf die *Folgen der Verweigerung der Einwilligung* in die Sicherheitsüberprüfung hinzuweisen. Allerdings ist lediglich der Hinweis enthalten, dass eine Sicherheitsüberprüfung undurchführbar ist, wenn der Betroffene oder sein Ehegatte/Lebenspartner die Einwilligung versagt. Dies widerspricht zum Teil der Rechtsprechung des Bundesverwaltungsgerichtes[95], wonach die Verweigerung der Einwilligung des Ehegatten/Lebenspartners in eine Speicherung seiner Daten in automatisierten Dateien nicht zu einer Undurchführbarkeit des Sicherheitsüberprüfungsverfahrens führt. Unserer Empfehlung, die Betroffenen auch hierauf hinzuweisen, wurde nicht gefolgt.

Die wesentlichen Maßnahmen bei der Durchführung der Sicherheitsüberprüfung werden nun zwar differenzierter dargestellt und damit die Transparenz des Verfahrens verbessert. Entgegen § 8 Abs. 1 BSÜG, wonach der Betroffene über Art und (tatsächlichen) Umfang der beabsichtigten Sicherheitsüberprüfung zu informieren ist, wird jedoch nur pauschal darüber unterrichtet, welche Maßnahmen ergriffen werden können. Die in § 8 Abs. 1 BSÜG vorgesehene Pflicht zur *Unterrichtung des Betroffenen über den Umfang der Datenerhebung* sollte auch sicherstellen, dass die später möglicherweise vorgenommene Befragung anderer Personen und Stellen (§ 13 Abs. 2 BSÜG) nur nach vorheriger Aufklärung und Einwilligung des Betroffenen erfolgt. Im Unterausschuss „Datenschutz“ hatte die Senatsverwaltung für Inneres zugesagt, dass der Betroffene abgestuft informiert wird über die von vornherein in jedem Fall erforderlichen Maßnahmen und über die später nach Lage des Einzelfalles gegebenenfalls noch nötigen Maßnahmen, über die der Betroffene dann allerdings ebenfalls zu unterrichten wäre. Letzteres ist nicht erfolgt.

In der vom Betroffenen und dem einbezogenen Ehegatten/Lebenspartner auszufüllenden Sicherheitserklärung befindet sich die Frage nach „sonstigen *Angaben mit Sicherheitsrelevanz“*. In den Ausfüllhinweisen wird darauf hingewiesen, dass alle Fragen zu beantworten sind. Da diese Frage nicht vom Gesetz gedeckt ist, kann sie allenfalls auf freiwilliger Basis beantwortet werden. Obwohl dies, wie zugesagt, in dem überarbeiteten Entwurf erfolgt ist, ist dieser Hinweis in der Ausführungsvorschrift wieder entfallen.

Nicht gefolgt wurde unseren Empfehlungen und den Empfehlungen des Unterausschusses „Datenschutz“ bei der *Konkretisierung der Sicherheitsrisiken.* In der Ausführungsvorschrift fehlt es an zusätzlichen Krite-

95 Beschluss vom 2. April 1996 (1 WB 71.95)

rien, in welchen Fällen die außereheliche intime Beziehung die Besorgnis der Erpressbarkeit begründet und objektiv zu einem Sicherheitsrisiko werden kann. In diesem Zusammenhang ist der Hinweis in den Ausführungsvorschriften bedenklich, dass eine Erpressbarkeit ausgeschlossen sei, wenn sich der Betroffene offen zu seinen Neigungen bekenne. In der Unterausschuss-Beratung wurde kritisiert, dass die Vorstellung, dass solche Beziehungen zwecks Abwehr der Erpressbarkeit dem Verfassungsschutz gemeldet werden sollten, grotesk sei.

Zusammenarbeit mit dem Verfassungsschutz

Ungeachtet weiterhin bestehender Dissenspunkte wie

- Umfang der Datenspeicherungen im NADIS[96],
- Kontrollkompetenz des Datenschutzbeauftragten bei der Verarbeitung von Daten, die durch G10-Maßnahmen erlangt wurden[97],
- Erfassung einfacher Mitglieder extremistischer Bestrebungen[98],
- Übermittlung und Speicherung der Daten von Demonstrationsteilnehmern[99],
- Auskunft auch ohne „berechtigtes Interesse“[99a]

ist eine konstruktive Zusammenarbeit mit dem Landesamt für Verfassungsschutz zu verzeichnen. Trotz unterschiedlicher Auffassungen zu Grundsatzfragen konnten in vielen Einzelfällen für Bürger, die sich an uns gewandt hatten, datenschutzrechtlich befriedigende Lösungen gefunden werden.

4.2 Ordnungsverwaltung

4.2.1 Gesetzgebung zur Verwaltungsreform

Das Zweite Gesetz zur Reform der Berliner Verwaltung vom 25. Juni 1998 (2. Verwaltungsreformgesetz – 2. VerwrefG)[100] sieht Änderungen zum Allgemeinen Zuständigkeitsgesetz (AZG) und zum Allgemeinen Sicherheits- und Ordnungsgesetz (ASOG) vor, die jeweils die *gegenseitigen Informationspflichten von Behörden* untereinander betreffen. Im Geltungsbereich des AZG betrifft dies die Senatsverwaltungen, Bezirksämter, Sonderbehörden und nichtrechtsfähigen Anstalten, im Geltungsbereich des ASOG gilt dies für die Ordnungsbehörden, nachgeordneten Ordnungsbehörden, die Polizei und die zuständigen Aufsichtsbehörden. Damit soll außerhalb der im Rahmen der Fachaufsicht (gewissermaßen „von unten nach oben“) bestehenden Informationspflicht ein darüber hinausgehender Informationsaustausch erfolgen und auf eine

96 JB 1996, 4.1.2
97 JB 1996, a.a.O
98 JB 1996, a.a.O
99 JB 1993, 4.5.2
99a JB 1993, 3.1
100 GVBl. S. 177

gesetzliche Grundlage gestellt werden. Wir haben im Rahmen der parlamentarischen Beratungen darauf hingewiesen, dass eine Weitergabe personenbezogener Daten von diesen Vorschriften nicht gedeckt und die Zulässigkeit nach den jeweils geltenden Befugnisregelungen zu beurteilen sei, und entsprechende Formulierungsvorschläge zur Ergänzung des Gesetzentwurfs unterbreitet. In der gemeinsamen Sitzung des Rechtsausschusses mit dem Ausschuss für Inneres, Sicherheit und Ordnung wurde festgestellt, dass unsere Ergänzungsvorschläge die (ohnehin geltende) Rechtslage wiedergeben, auf die im Gesetz selbst nicht nochmals hingewiesen werden müsse. Unsere Empfehlung wurde als Hinweis des Berliner Datenschutzbeauftragten auf die geltende Rechtslage als Protokollnotiz aufgenommen und von den Ausschussmitgliedern „ausdrücklich zur Kenntnis genommen“.

Ein zwischenzeitlich vorgelegter Entwurf über ein „Drittes Gesetz zur Reform der Berliner Verwaltung“ (Verwaltungsreform-Grundsätze-Gesetz – VGG) wird derzeit in den parlamentarischen Ausschüssen behandelt. Die dort genannten Reformmaßnahmen sollen die Basis für eine grundlegende Reorganisation der Berliner Verwaltung sein zur Verbesserung ihrer Wirtschaftlichkeit und Wirksamkeit. Wesentliche Konzeption des Gesetzentwurfs ist u. a. die stärkere Berücksichtigung der Bedürfnisse des Bürgers als Adressat des Verwaltungshandelns. Geplant ist, diese Bedürfnisse z. B. mit *Kundenbefragungen* zu analysieren. Da die vorgesehene Bestimmung offen ließ, ob diese Befragungen anonym oder personenbezogen durchgeführt werden sollen, haben wir empfohlen, eine Ergänzung dahingehend vorzunehmen, dass die Adressaten auf die Freiwilligkeit und die Möglichkeit der anonymen Beantwortung hinzuweisen sind.

Der Entwurf des VGG sieht auch eine Änderung des Bezirksverwaltungsgesetzes vor, nach der die Bezirksämter neu strukturiert werden sollen. Publikumsintensive Leistungen verschiedener Fachämter werden künftig gebündelt und dem Bürger in einem Bürgeramt angeboten. Unsere Anregung, die *Übertragung hoheitlicher Befugnisse vom Fachamt auf das neue Bürgeramt* auf eine gesetzliche Grundlage zu stellen, ist im Gesetzentwurf ebenso berücksichtigt worden wie unsere Empfehlung, eine spezialgesetzliche Befugnisnorm vorzusehen, die einerseits die Datenverarbeitung ausserhalb der fachlich zuständigen Organisationseinheit zulässt, anderseits aber klarstellt, dass die Datenverarbeitung nicht über dasjenige hinausgehen darf, was für die jeweilige Organisationseinheit nach den jeweils geltenden Befugnisregelungen zulässig ist. In dem im neuen Jahr in das Abgeordnetenhaus eingebrachten Entwurf ist überraschenderweise zusätzlich vorgesehen, dass im Rahmen einer „Experimentierklausel“ eine Reihe von Aufgaben des Landeseinwohneramtes (LEA) auf die Bürgerämter übertragen werden soll. Umgekehrt sollen Mitarbeiter des LEA mit einzelnen bezirklichen Aufgaben betraut werden. Inwieweit dies mit dem Datenschutzrecht vereinbar ist, ist noch offen.

Bei der im VGG vorgesehenen *„übergreifenden Personalplanung“* haben wir empfohlen klarzustellen, dass der hierfür zuständigen Senatsverwaltung von den jeweiligen Organisationseinheiten aggregierte (also nicht personenbezogene) Informationen zur Verfügung gestellt werden.

Durch eine Änderung der Landeshaushaltsordnung soll die *Senatsverwaltung für Finanzen* „unter Beachtung datenschutzrechtlicher Vorschriften“ von allen Stellen der Berliner Verwaltung *Auskünfte und die Vorlage von Unterlagen* verlangen können. Wir haben darauf hingewiesen, dass wegen der Verweisung auf spezialrechtliche Regelungen in § 6 Abs. 1 Berliner Datenschutzgesetz die LHO selbst den Umfang der Daten bestimmen muss und darüber hinaus ein klarer Hinweis erforderlich ist, dass die Bestimmung nur für die eigenen Aufgaben der Senatsverwaltung für Finanzen gelten soll. Da entsprechende Befugnisse auch der für die Personalwirtschaft und die Stellenpläne zuständigen Senatsverwaltung zustehen sollen, hielten wir einen Verweis auf die speziellen datenschutzrechtlichen Bestimmungen des Landesbeamtengesetzes (§§ 56 ff.) für erforderlich.

4.2.2 Meldewesen, Wahlen, Standesämter

Meldewesen und Wahlen

Der lange angekündigte Entwurf eines *Meldegesetzes,* der die Änderung des Melderechtsrahmengesetzes umsetzt und die von uns seit langem geforderten Klarstellungen im bestehenden Melderecht berücksichtigt[101], wurde wiederum nicht vorgelegt. Nachdem auch in Brandenburg ein Gesetzentwurf im Landtag eingebracht wurde, bildet Berlin hinsichtlich der Fortentwicklung des Melderechtes nun das Schlusslicht.

> *Empörung hat auch in Berlin ausgelöst, dass in den Landtagswahlkämpfen in Hamburg und Sachsen-Anhalt eine rechtsradikale Partei in massiver Weise die Wählerlisten genutzt hat, die ihr nach dem dortigen Meldegesetz übergeben worden waren.*

Anträge der Fraktion Bündnis 90/Die Grünen[102], das Melderechtsrahmengesetz und das Meldegesetz dahingehend zu ändern, dass *Auskünfte aus dem Melderegister zum Zweck der Wahlwerbung* an die Parteien, Wählergemeinschaften und Einzelbewerber im Vorfeld von Wahlen nur noch nach ausdrücklicher Einwilligung der Betroffenen zulässig sind, wurden vom Abgeordnetenhaus abgelehnt. Damit würde verhindert werden, dass bei den Parteien umfangreiche Datenbestände entstehen. Zwar haben die Parteien diese Daten eine Woche nach der Wahl zu löschen und entsprechende Verpflichtungserklärungen abzugeben, kontrollieren kann das die Aufsichtsbehörde allerdings nur schwer.

[101] JB 1997, 4.2.1
[102] Abghs. Drs. 13/2987 und 13/2988

Nach § 38 Abs. 1 BDSG müssen hinreichende Anhaltspunkte für eine Datenschutzverletzung vorliegen. Eine Überprüfung ohne Anlass ist hier nicht möglich.

Nicht zuletzt aus diesem Grund hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den gesetzgebenden Körperschaften empfohlen, die Einwilligungslösung vorzuziehen[103].

Standesämter

Am 1. Juli 1998 ist das Gesetz zur Neuordnung des Eheschließungsrechtes in Kraft[104] getreten, das verschiedene datenschutzrechtlich relevante Änderungen enthält. Nach dem neu gefassten § 1314 Bürgerliches Gesetzbuch (BGB) kann eine Ehe aufgehoben werden, wenn beide Ehegatten sich bei der Eheschließung darüber einig waren, dass sie keine eheliche Lebensgemeinschaft begründen wollen. Wenn für eine derartige *„Scheinehe“* konkrete Anhaltspunkte bestehen, hat der Standesbeamte das Recht, die Verlobten zu befragen (§ 5 Abs. 4 Personenstandsgesetz [PStG]). Er kann die Beibringung geeigneter Nachweise und notfalls eine eidesstattliche Versicherung über Tatsachen verlangen, die für die Feststellung, ob eine „Scheinehe“ vorliegt, von Bedeutung sind. Diese Neuregelungen zielen darauf ab, „Scheinehen“ von ausländischen Staatsangehörigen zu verhindern, die zum Erwerb eines Aufenthaltsrechtes geschlossen werden.

Der Standesbeamte darf die Verlobten nur *befragen,* wenn Tatsachen vorliegen, die konkret den Verdacht einer Scheinehe begründen. Vermutungen sind nicht ausreichend. Der Standesbeamte darf nicht die Motive der Eheschließenden von sich aus inquisitorisch erforschen und ihnen peinliche und entwürdigende Fragen stellen und ihnen den Eindruck vermitteln, sie müssten vorbehaltlos darlegen, dass es sich bei ihrer Ehe nicht um eine Scheinehe handelt[105].

Bei der Frage, ob konkrete Anhaltspunkte für eine „Scheinehe“ vorliegen, sind die unterschiedlichen Lebensformen zu berücksichtigen. Ein großer Altersunterschied reicht ebenso wenig aus wie das Fehlen einer häuslichen Gemeinschaft. Eine lebenslange Partnerschaft kann ersichtlich auch von verschieden alten Partnern angestrebt werden; auch die bestehende häusliche Gemeinschaft sagt nichts über die Ernsthaftigkeit der Partnerschaft aus. Der Wille zu einer lebenslangen Beziehung setzt keinen gemeinsamen Wohnsitz voraus. Das Verwaltungsgericht Berlin hat dazu ausgeführt, dass es so sein mag, dass die häusliche Gemeinschaft zu dem in der Regel vorkommenden Merkmal ehelicher Lebensführung in der Gesellschaft zählt. Daraus kann jedoch nicht

[103] Anlagenband „Dokumente zum Datenschutz 1998“, Teil B III
[104] BGBl. I S. 833
[105] BVerfGE 76, 1, 61

geschlossen werden, dass eine eheliche Lebensgemeinschaft ohne häusliche Gemeinschaft nicht mehr die sittlichen und gesellschaftlichen Merkmale des Ehestandes aufweise[106].

Auch das Fehlen einer Aufenthaltsgenehmigung kann die Ermittlungsbefugnisse des Standesbeamten nicht auslösen, denn eine lebenslange Partnerschaft kann auch dann gewollt sein, wenn einem Partner eine ausländerrechtliche Genehmigung zur Zeit der Eheschließung fehlt.

Konkrete Anhaltspunkte liegen z. B. vor, wenn der Standesbeamte erfahren hat, dass die Eheleute keine partnerschaftliche Beziehungen pflegen wollen, insbesondere wenn der eine Teil dies erklärt hat. Dies kann sich daraus ergeben, dass der eine Partner den anderen praktisch nicht kennt, für seine Bereitschaft zur Eheschließung Geld gefordert oder genommen hat oder sich überhaupt nicht mit dem anderen verständigen kann. Nur in derartigen Fällen hat der Standesbeamte auch das Recht, weitere Ermittlungen anzustellen und auch den Aufenthaltsstatus zu ermitteln. Ansonsten ist für seine Amtsgeschäfte lediglich der Nachweis der Staatsangehörigkeit nötig, der durch Passvorlage oder Beibringung einer entsprechenden Urkunde geleistet werden kann (§ 11 Abs. 2 PStG).

Das Bezirksamt Spandau hat ein eigenes DV-Programm „Einbürgerung" entwickelt. Damit werden verschiedene Statistiken als personenbezogene Auflistungen erstellt, die wahlweise auch nach dem Namen des Antragstellers sortiert werden können.

Die Grundlage für diese Datenaufbereitung ist ein Schreiben der Senatsverwaltung für Inneres, wonach von den Standesämtern personenbezogene *Eingangs-, Erledigungs- und Gesamtstatistiken* als Auflistungen von Einzeldatensätzen mit festgelegten personenbezogenen Merkmalen wie Name, Herkunftsland und Aktenzeichen zu führen und diese quartalsweise der Senatsverwaltung für Inneres zu übersenden sind. Diese Listen werden durch das Programm „Einbürgerung" erstellt und gedruckt.

Hier wurde allerdings weder eine Statistik erstellt noch eine solche an die Senatsverwaltung für Inneres übermittelt. Der Begriff „Statistik" ist an dieser Stelle irreführend. Das Bezirksamt hat in Staatsangehörigkeitsangelegenheiten – als Bezirksaufgaben unter Fachaufsicht – die Zuständigkeit für Anspruchseinbürgerungen sowie Mitwirkung bei Ermessenseinbürgerungen. Hierfür können von dem Bezirksamt personenbezogene Daten erhoben und gespeichert werden. Personenbezogene Daten dürfen nach §§ 11, 12 BlnDSG grundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben oder gespeichert worden sind. Sollen personenbezogene Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder gespeichert wurden, so ist dies außer im Fall der Einwilligung nur zulässig, wenn eine ausdrückliche Rechtsgrundlage hierfür vorliegt. Da dies nicht der Fall ist, hat das Standesamt personenbezogene Einzeldaten aus der Vorgangsbearbeitung zu Staatsangehörigkeitsangelegenheiten rechtswidrigerweise an die Senatsverwaltung für Inneres übermittelt. Wir haben das Verfahren beanstandet. Die personenbezogenen Übermittlungen sind inzwischen eingestellt worden. Die Senatsverwaltung für Inneres hat mit Rundschreiben die Einbürgerungsbehörden angewiesen, keine Indexkarten, Schlussmitteilungen oder sonstige Verfahrensabschlüsse und Übernahme- oder Abgabenachrichten dorthin zu senden.

106 VG Berlin, NJWE-MietR 1997, 284

4.2.3 Ausländerangelegenheiten

Ausländische Gäste

Der Gastgeber eines ausländischen Besuchers hat sich zu verpflichten, für alle Kosten aufzukommen, die durch den Aufenthalt seines Gastes entstehen (§ 84 Ausländergesetz [AuslG]). Bereits im vergangenen Jahr[107] haben wir über die erheblichen datenschutzrechtlichen Bedenken berichtet, die gegen das bundeseinheitliche Formular – mit dem umfangreiche Daten zur Person der Gastgeber erhoben werden – bestehen.

Diese Bedenken wurden zum Teil bei der Neufassung der „Hinweise zur Verwendung des bundeseinheitlichen Formulars der *Verpflichtungserklärung"* berücksichtigt. Eine Umgestaltung des Formulars für die Abgabe einer Verpflichtungserklärung wird derzeit überprüft.

Der Empfehlung, die Angabe des Berufes und des Arbeitgebers zu streichen, wurde nicht gefolgt. Der Verzicht auf eine Eintragung im Feld „Bemerkungen", dass gegen die Einreise des Ausländers keine Bedenken bestehen – wodurch deutlich wird, dass es sich bei dem Einladenden um einen Sozialhilfeempfänger handelt –, wurde ebenfalls nicht umgesetzt. Missverständlich ist der Hinweis, dass zukünftig auf Detailangaben zu Wohn-, Einkommens- und Vermögensverhältnissen des Gastgebers im Regelfall verzichtet werden sollte. Hier hätte der Hinweis erfolgen müssen, dass auf Detailangaben in jedem Fall zu verzichten ist.

Wir haben empfohlen, beim Ausfüllen des Vordruckes auf Eintragungen in den Rubriken

- Beruf,
- Mieter/Eigentümer,
- Arbeitgeber,

107 JB 1997, 4.2.2

– sonstige Angaben zu den Wohn-, Einkommens- und Vermögensverhältnissen (Größe der Wohnung, Höhe des Einkommens)

vollständig zu verzichten. Die Senatsverwaltung für Inneres hat diese Empfehlung aufgegriffen und die Ausländerbehörde gebeten, bei Verwendung der Vordrucke bis zu deren datenschutzgerechten Überarbeitung auf Eintragungen in den genannten Feldern zu verzichten. Wir gehen davon aus, dass die Bearbeitungshinweise für die Entgegennahme von Verpflichtungserklärungen in der Ausländerbehörde entsprechend modifiziert werden.

Auskunftsersuchen der Ausländerbehörde an die Hochschulen zur Abgabe einer Studienprognose

Zur Verlängerung von Aufenthaltsbewilligungen ausländischer Studenten bittet die Ausländerbehörde die Berliner Hochschulen um die Abgabe einer Studienprognose.

Die Verlängerung einer Aufenthaltsbewilligung wird nach § 28 Abs. 1 AuslG erteilt, wenn der Ausländer nur für einen bestimmten, seiner Natur nach nur einen vorübergehenden Aufenthalt erfordernden Zweck die Genehmigung begehrt. § 28 Abs. 2 Satz 2 AuslG bestimmt, dass die Verlängerung erteilt werden kann, wenn der Aufenthaltszweck noch nicht erreicht ist und in einem angemessenen Zeitraum noch erreicht werden kann. Dazu ist bei Studierenden eine Prognose der Ausländerbehörde nötig, die sich an dem erkennbaren Bemühen des Ausländers, das Ziel seines Aufenthaltes in einem überschaubaren Zeitraum zu erreichen, auszurichten hat, so dass die Erwartung gerechtfertigt ist, dass er in absehbarer Zeit wieder in sein Heimatland zurückkehren kann. Für diese Prognose ist es offensichtlich notwendig, Aufschluss über den Studienverlauf des Ausländers zu erlangen. Damit erfolgt die beabsichtigte Datenerhebung zu einem zulässigen Zweck nach § 75 Abs. 1 AuslG.

Die Daten sind grundsätzlich bei dem Betroffenen zu erheben (§ 75 Abs. 2 Satz 2 Nr. 3 erste Alt. AuslG). Ohne Mitwirkung des Betroffenen dürfen Daten über ihn erhoben werden, wenn die Mitwirkung des Betroffenen nicht ausreicht (§ 75 Abs. 2 Satz 2 Nr. 3 erste Alt. AuslG). Der Betroffene kann die erforderlichen Informationen selbst erbringen. Die *Vorlage des Studienbuches* gibt Aufschluss über Semesteranzahl, Veranstaltungen usw.. Leistungsnachweise können das Erreichen von Studienzielen dokumentieren. Ein Abgleich mit einem Studienplan und der Regelstudienzeit kann der Ausländerbehörde das Verhältnis des individuellen Studiengangs zu den allgemeinen Anforderungen erschließen.

Die Anforderung einer Studienprognose erscheint nur sinnvoll, wenn in einem Ausnahmefall Regelstudienzeiten überschritten oder Ausbildungsziele nicht erreicht wurden, um nachzuweisen, dass ein Erreichen

des Ausbildungszieles dennoch möglich ist. In diesen Fällen kann die Studienprognose jedoch vom Betroffenen selbst beantragt und beigebracht werden. Eine entsprechende Beibringungspflicht regelt § 70 AuslG.

Die Mitwirkung des Betroffenen stellt auch keinen unverhältnismäßigen Aufwand dar (§ 75 Abs. 2 Satz 2 Nr. 3 zweite Alt. AuslG). Dazu muss ein markantes Missverhältnis zwischen Aufwand der Datenerlangung und der Bedeutung der Sache bestehen. Bloße Arbeitserschwernis, Umständlichkeit des Verfahrens oder geringfügige Verzögerungen im Ablauf reichen hier nicht aus. Es ist nicht ersichtlich, warum die genannten Unterlagen vom Betroffenen nicht schnell und ohne Aufwand beigebracht werden könnten.

Mitwirkung der Ausländerbehörde bei der Erteilung von iranischen Reisepässen

Einem ausreisewilligen iranischen Asylbewerber wurde durch die Ausländerbehörde eines anderen Bundeslandes zur Beschaffung von Ausreisepapieren (Passbeschaffung) ein Erhebungsbogen der Iranischen Botschaft in Bonn zum Ausfüllen vorgelegt, der Fragen enthält, die nach deutschem Recht als bedenklich anzusehen sind. Dies erfolgte, obwohl die Iranische Botschaft auch einen Fragebogen zur Ausstellung eines Rückreisescheines (Passierscheines) für die Einreise in den Iran bereithält, der nur noch Fragen enthält, die auch mit dem deutschen Recht zu vereinbaren sind.

Mit der Erteilung eines derartigen *Rückreisescheines* wird bereits die von der Ausländerbehörde angeordnete Ausreise des Ausländers ermöglicht. Die Beantragung eines Reisepasses und die damit verbundene unzulässige Befragung ist für die Ausreise iranischer Bürger somit nicht erforderlich.

Unsere Nachfrage zur Berliner Vorgehensweise ergab, dass die Berliner Ausländerbehörde in den genannten Fällen ein Antragsformular verwendet, das dem „Fragebogen für die Ausstellung eines Rückreisescheines“ der Iranischen Botschaft inhaltlich weitgehend entspricht und das nur Daten enthält, die keinen datenschutzrechtlichen Bedenken begegnen.

4.2.4 Verkehr

Am 1. Januar 1999 ist das Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze in Kraft[108] getreten. Über den jeweiligen Stand des Gesetzgebungsverfahrens und die wesentlichen datenschutzrelevanten Änderungen haben wir seit 1993 kontinuierlich berichtet[109].

[108] BGBl. I
[109] zuletzt JB 1997, 4.2.3

Als wesentliche Neuerungen nochmals hervorzuheben sind die Regelungen über den Umgang mit Daten in der Führerscheinakte, insbesondere über die *Vernichtung von Unterlagen* (z. B. Registerauskünften, Führungszeugnissen, Gutachten und Gesundheitszeugnissen). Spätestens fünfzehn Jahre nach In-Kraft-Treten des Gesetzes sollen alle Akten „auf Vernichtenswertes“ überprüft sein.

Wir haben seit Monaten darauf hingewiesen, dass die Berliner Führerscheinstelle als diejenige Stelle, die die Bereinigung der Führerscheinakten vorzunehmen hat, angesichts der Vielzahl dieser Akten frühzeitig – und nicht erst bei In-Kraft-Treten des Gesetzes – mit der Umsetzung der neuen Bestimmungen beginnt. Der Unterausschuss „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung ist unserer Auffassung gefolgt und hat bereits Ende 1997 den Senat aufgefordert, die vom Bundestag schon beschlossenen Aktenbereinigungsfristen umzusetzen. Der Senat ist dieser Aufforderung nicht nachgekommen, er hat die vom Gesetzgeber vorgesehene Frist von acht Monaten bis zum In-Kraft-Treten des Gesetzes ungenutzt verstreichen lassen und keinen allgemeinen Verfahrensvorschlag dafür vorgesehen, wie der einzelne Mitarbeiter in der Führerscheinstelle die Bereinigung einer Akte im Einzelfall vorzunehmen hat.

In der erneut anberaumten Sitzung des Unterausschusses „Datenschutz“ Ende 1998 haben die Fraktionen übereinstimmend die „völlig unzulängliche Vorbereitung der Verwaltung auf die neue Rechtslage“ kritisiert, die „schon seit Monaten so erwartet worden“ sei. Der Ausschuss hält – ebenso wie wir – eine Arbeitsanweisung zur Umsetzung der neuen Tilgungsfristen im Interesse eines einheitlichen Verwaltungshandelns für unerlässlich und bezeichnet es als „nicht nachvollziehbar, dass die Verwaltung auf ein solches Papier offenbar verzichten wolle“.

In einer weiteren Sitzung des Unterausschusses im neuen Jahr sicherte die Senatsverwaltung für Bauen, Wohnen und Verkehr daraufhin zu, die Umsetzung der neuen Rechtslage unverzüglich in Angriff zu nehmen und eine entsprechende Arbeitsanweisung zu erstellen.

4.3 Justiz und Finanzen

4.3.1 Justiz

In Kraft getreten ist das Justizmitteilungsgesetz, verabschiedet wurden das Vierte Strafvollzugsänderungsgesetz (StVollzÄndG) und das DNA-Identitätsfeststellungsgesetz, die beide auch 1998 in Kraft getreten sind[112]. Nicht zum Abschluss gebracht hat der Gesetzgeber in der vergangenen Ligistlaturperiode das Strafverfahrensänderungsgesetz (StVÄG) 1996, über das wir schon mehrfach berichtet haben[113]. Dies bedeutet, dass in einem wichtigen Bereich der Justiz auch weiterhin ohne ausreichende datenschutzrechtliche Regelungen gearbeitet werden muss. Inzwischen hat die Bundesregierung den Entwurf eines StVÄG 1999 vorgelegt[114].

Das *Justizmitteilungsgesetz* (JuMiG)[115] ist am 1. Juni 1998 in Kraft getreten. Dadurch wird erstmals in Form eines Gesetzes geregelt, in welchen Fällen personenbezogene Mitteilungen der Justizbehörden über staatsanwaltschaftliche und gerichtliche Verfahren an andere öffentliche Stellen zulässig sind. Nicht aufgenommen wurde allerdings die Pflicht zur *Benachrichtigung des Betroffenen* über die Datenübermittlungen. Nur in den Fällen, in denen der Betroffene bei Mitteilungen in Strafsachen nicht zugleich der Beschuldigte oder in Zivilsachen nicht zugleich Partei oder Beteiligter ist, sieht das Gesetz eine Unterrichtung über den Inhalt und den Empfänger der Mitteilung von Amts wegen vor. In allen übrigen Fällen wird dem Betroffenen nur auf Antrag Auskunft erteilt.

Vor dem In-Kraft-Treten des Gesetzes sind die *Verwaltungsvorschriften über Mitteilungen in Strafsachen und Zivilsachen* (MiStra und MiZi) von den Justizverwaltungen des Bundes und der Länder den Regelungen des JuMiG angepasst worden. Die von den Datenschutzbeauftragten angeregten Änderungen sind nur zum Teil aufgegriffen worden.

So wurde klargestellt, dass der *automatisierte Abruf* von Informationen durch die empfangenden Stellen unzulässig ist (Nr. 9 Abs. 2 MiStra). Nach § 15 Abs. 1 BlnDSG darf ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte nur eingerichtet werden, wenn ein Gesetz dies ausdrücklich zulässt. Das JuMiG lässt einen automatisierten Abruf nicht zu. Die MiStra als bloße Justizverwaltungsvorschrift reicht zur Einrichtung eines automatisierten Abrufverfahrens nicht aus.

---

112 vgl. 1.1
113 JB 1996, 4.3.1; JB 1997, 4.3.1
114 BR-Drs. 65/99
115 BGBl. 1997 I S. 1430; vgl. auch JB 1997, 4.3.1, und JB 1996, 4.3.1

Unverändert hingegen blieb die Regelung in den Mitteilungen in Strafsachen (z. B. in Nr. 6 Abs. 4 und 5 MiStra), die vollständige Anklageschrift bzw. das vollständige Urteil mitzuteilen. Nur im Einzelfall kann angeordnet werden, dass die Übermittlung des wesentlichen Ergebnisses der Ermittlungen oder die Übermittlung der Urteilsgründe unterbleiben sollen. Das in dieser Vorschrift vorausgesetzte Regel-Ausnahme-Verhältnis basiert auf einer pauschalen Vermutung zugunsten der Erforderlichkeit einer vollständigen Übermittlung. Der Grundsatz der Verhältnismäßigkeit gebietet jedoch eine Erforderlichkeitsprüfung nicht nur bezüglich der Mitteilung als solcher, sondern auch hinsichtlich ihres konkreten Umfanges. Mitteilungen in Strafsachen zeichnen sich durch einen hohen Grad an Sensibilität und Schutzwürdigkeit der zu übermittelnden personenbezogenen Daten aus. Deshalb sollte im Einzelfall geprüft werden, ob über die Mitteilung des Anklagesatzes oder der Urteilsformel hinaus die *Mitteilung der vollständigen Anklageschrift* bzw. der Urteilsgründe erforderlich ist.

Neben den MiStra waren auch die *Richtlinien für das Straf- und Bußgeldverfahren* (RiStBV) zu überarbeiten. Das JuMiG hat den § 8 in das Einführungsgesetz zur Strafprozessordnung (EGStPO) eingeführt. Danach ist in Strafsachen gegen Mitglieder der gesetzgebenden Körperschaften dem Präsidenten der Körperschaft, der das Mitglied angehört, die das Verfahren abschließende Entscheidung einschließlich ihrer Begründung zu übermitteln. Entgegen dieser Regelung sieht Nr. 192 Abs. 5 RiStBV[116] jetzt vor, dass diese Mitteilung auf dem Dienstweg zu erfolgen hat. Da nach dem Wortlaut des § 8 EGStPO die Mitteilung an den Präsidenten der gesetzgebenden Körperschaft zu richten ist, findet Nr. 192 Abs. 5 RiStBV im Gesetz keine Stütze. Darüber hinaus ist nach Nr. 10 Abs. 2 MiStra für andere Berufsgruppen in Strafsachen grundsätzlich sicherzustellen, dass die Mitteilungen unmittelbar die bei der empfangenden Stelle funktionell zuständigen Bediensteten erreicht. Da die Mitteilung über den Dienstweg zur Folge hätte, dass einer Vielzahl von Stellen ohne gesetzliche Grundlage höchst sensible Daten aus *Strafverfahren gegen Abgeordnete* zur Kenntnis gebracht würden, empfehlen wir, von dem Vollzug der Nr. 192 Abs. 5 RiStBV abzusehen. Der Präsident des Abgeordnetenhauses kann im Übrigen nach § 8 Abs. 2 EGStPO auf die Übermittlung der abschließenden Entscheidung verzichten. Die Senatsverwaltung für Justiz ist der Ansicht, die Übermittlung der das Verfahren endgültig abschließenden Entscheidung sei im Wege der Ausübung der Dienst- und Fachaufsicht nach §§ 145 bis 147 GVG i.V.m. § 21 Abs. 1 AGGVG zulässig. Erforderlich ist es für die Fachaufsicht jedoch nur, den Stellen, die auf dem Dienstweg Kenntnis von dem Antrag zur Aufhebung der Immunität erlangt haben (Nr. 192 Abs. 3 RiStBV), mitzuteilen, dass das Verfahren durch Einstellung oder Urteil geendet hat. Nicht erforderlich ist die Übermittlung der Entscheidungsgründe, da damit jedenfalls in den Fällen, in denen die Unschuld des betroffenen Abgeordneten nicht zweifelsfrei festgestellt werden konnte, ein schwerwiegender Eingriff in dessen Persönlichkeitsrecht verbunden ist.

[116] ABl. 1998, S. 2240

Nach Nr. IV/1 der *Mitteilungen in Zivilsachen* (MiZi) ist dem Sozialamt der Eingang einer Klage mitzuteilen, mit der die Räumung von Wohnraum im Fall der Kündigung des Mietverhältnisses wegen Zahlungsverzuges des Mieters nach § 554 BGB verlangt wird. Diese Mitteilungspflicht beruht auf § 15 a Bundessozialhilfegesetz (BSHG), wonach Hilfe zum Lebensunterhalt gewährt werden kann, wenn dies zur Sicherung der Unterkunft gerechtfertigt ist. Auf Anregung der Datenschutzbeauftragten wurde vorgesehen, dass der Betroffene gleichzeitig mit der *Unterrichtung des Sozialamtes* hierüber zu unterrichten ist. Nicht in jedem Fall einer *Räumungsklage* ist Ursache des Zahlungsverzuges die Zahlungsunfähigkeit des Mieters. Der Zahlungsverzug kann z. B. auch auf eine Minderung des Mietzinses zurückzuführen sein. Die tatsächliche Ursache wird sich häufig nicht bereits aus der Klageschrift ergeben. Die Sozialämter werden daher über eine nicht unerhebliche Zahl von Räumungsklagen informiert, obwohl die Mitteilung nicht in jedem Fall für ihre Aufgabenerfüllung erforderlich ist und die Mitteilung an die Sozialbehörde darüber hinaus sogar erheblichen Interessen der beklagten Mieter widersprechen kann. Durch die Unterrichtung wird dem Betroffenen in diesen Fällen zumindest die Möglichkeit eröffnet, von sich aus auf eine Löschung der überflüssigerweise übermittelten Daten hinzuwirken, bevor das Sozialamt weitere Aktivitäten entwickelt.

Nach Nr. I/11 Abs. 1 Nr. 1 MiZi hat das Gericht der *Ausländerbehörde* den „Aufenthalt“ eines Ausländers mitzuteilen, der weder eine erforderliche Aufenthaltsgenehmigung noch eine Duldung besitzt. Diese Verwaltungsvorschrift – deren Zweck es auch sein sollte, die praktische Umsetzung der in § 76 Abs. 2 Nr. 1 Ausländergesetz (AuslG) geregelten Mitteilungspflicht zu erleichtern – gibt lediglich dessen Wortlaut wieder. Die Mitteilungspflicht umfasst nur die Mitteilung der Tatsache, dass der Betroffene sich unberechtigterweise in der Bundesrepublik aufhält. Unserem Vorschlag klarzustellen, dass lediglich die Identifizierungsdaten eines Ausländers sowie die Tatsache seines unerlaubten Aufenthaltes mitzuteilen sind, wurde nicht gefolgt.

Neue Datenschutzregelungen für den Strafvollzug

Am 1. Dezember 1998 ist das Vierte Gesetz zur Änderung des Strafvollzugsgesetzes[117] in Kraft getreten, das die Datenverarbeitung im Strafvollzug[118] auf eine bereichsspezifische Rechtsgrundlage stellt.

[117] BGBl. I, S. 2461
[118] vgl. JB 1995, 3.4

Im vergangenen Berichtsjahr haben wir die Gespräche mit der Leitung der JVA Tegel zur Abarbeitung der bei unserer 1995 durchgeführten Querschnittsprüfung festgestellten datenschutzrechtlichen Probleme fortgesetzt[119]. Im Mittelpunkt stand dabei die Datenverarbeitung in den *Arztgeschäftsstellen* der Teilanstalten. Bei unserer Prüfung hatten wir festgestellt, dass auf zahlreichen Krankenakten ein „roter Punkt" angebracht worden war. Dieser soll darauf hinweisen, dass der Gefangene HIV-infiziert ist. Mit der JVA Tegel wurde vereinbart, dass diese „roten Punkte" entfernt werden. Durch dieses Kennzeichen wird schon von weitem – insbesondere bei etwaigen Aktentransporten – das Vorliegen eines Sondermerkmales signalisiert und dadurch auch für den Transport ein zusätzliches Risiko für eine unbefugte Offenbarung dieser sehr sensiblen Angabe geschaffen. Die Markierung durch einen „roten Punkt" widerspricht auch dem Verhältnismäßigkeitsgrundsatz, da sie dem Patienten schon optisch das Gefühl einer Stigmatisierung vermittelt, wenn dieser bei der Behandlung die Unterlagen zu Gesicht bekommt, und auch für andere in den Behandlungsraum Eintretende dieses Merkmal ohne große Schwierigkeiten erkennbar sein kann. Diese Auffassung wird auch von der Ärztekammer Berlin geteilt. Nach deren Ansicht geht diese Form der Kennzeichnung auch über eine sinnvolle und notwendige Information der nachbehandelnden Ärzte hinaus.

Auch die regelmäßige – d. h. unabhängig von einer konkret bevorstehenden Behandlung – *Mitteilung über HIV-infizierte Gefangene* an den Zahnarzt der Anstalt und die regelmäßige Übermittlung dieses Hinweises an mit- oder nachbehandelnde Ärzte, die in der Vergangenheit in der JVA Tegel praktiziert wurde, ist unzulässig. Patientendaten dürfen nur an andere Ärzte weitergegeben werden, wenn dies zur Nach- und Weiterbehandlung erforderlich ist (§§ 3 Abs. 4 und 6, 4 Abs. 3 Berufsordnung der Ärzte i.V.m. §§ 6, 13 BlnDSG). Dies gilt für alle Patienten, also auch für Gefangene in einer Justizvollzugsanstalt.

DNA-Identitätsfeststellungsgesetz

Als Abschiedsgeschenk hat die alte Bundesregierung noch das DNA-Identitätsfeststellungsgesetz vom 7. September 1998[120] hinterlassen. Dieses Gesetz ergänzt zunächst die Strafprozessordnung um einen § 81 g. Diese Vorschrift regelt, dass dem Beschuldigten, der einer Straftat von erheblicher Bedeutung – insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung – verdächtig ist, zum Zweck der *Identitätsfeststellung* in künftigen Strafverfahren Körperzellen entnommen und zur Feststellung des *DNA-Identifizierungsmusters* molekulargenetisch untersucht

[119] JB 1995, 3.5; JB 1997, 4.3.1
[120] BGBl. I S. 2646

werden dürfen, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Täters oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer der genannten Straftaten zu führen sind. Nach § 2 DNA-Identitätsfeststellungsgesetz ist die Durchführung solcher Maßnahmen auch dann zulässig, wenn der Betroffene wegen einer der genannten Straftaten rechtskräftig verurteilt oder nur wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit, auf Geisteskrankheit beruhender Verhandlungsunfähigkeit oder fehlender oder nicht ausschließbarer fehlender Verantwortlichkeit (§ 3 JGG) nicht verurteilt worden ist und die entsprechende Eintragung im Bundeszentralregister oder Erziehungsregister noch nicht getilgt ist. Darüber hinaus regelt das Gesetz, dass die so gewonnenen Daten nach dem Bundeskriminalamtsgesetz in einer zentralen Datei bei dem BKA verarbeitet und genutzt werden können.

Diese Möglichkeit des Vorhaltens hochsensibler personenbezogener Informationen in einer Datei stellt einen Eingriff in das Persönlichkeitsrecht von völlig neuer Qualität dar. Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit zwar noch keine über die Identifizierung hinausgehenden *Aussagen zur jeweiligen Person oder zu deren Erbgut;* in Einzelfällen können die analysierten, nicht-codierenden, persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten, intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, dass künftig auch auf der Basis der Untersuchung von bisher als nichtcodierend angesehenen Merkmalen konkrete Aussagen mit inhaltlichem Informationswert über genetische Dispositionen der betroffenen Personen getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten medizinischen Genoms vorangetrieben wird. Dieser Gefährdung hätte dadurch begegnet werden können, dass bei Bekanntwerden von Überschussinformationen durch die bisherigen *Untersuchungsmethoden* andere Untersuchungmethoden – z. B. die Analyse eines anderen Genom-Abschnittes – verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, dass die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse können daher dazu führen, dass einmal verwendete Untersuchungsmethoden im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat darauf hingewiesen, dass – wenn man dieses Risiko dennoch hinnimmt – zumindest ein grundsätzliches *Verbot der Verformelung* und

Speicherung solcher Analyse-Ergebnisse statuiert werden müsse, die inhaltliche Aussagen über Erbanlagen ermöglichen[121]. Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen hätte ein striktes *Nutzungsverbot* statuiert werden müssen für persönlichkeitsrelevante Erkenntnisse, die aus den gespeicherten Verformelungen der DNA resultieren. Dem ist der Gesetzgeber nicht nachgekommen.

Auch im Übrigen bieten die einzelnen Vorschriften Anlass zur Kritik:

- Der *Straftatenkatalog* des § 81 g Abs. 1 StPO ist zu weit gehend. Wegen der besonderen Eingriffsqualität kann die Speicherung von DNA-Analyseergebnissen nur gerechtfertigt sein bei Beschuldigten, die eines Verbrechens gegen Leib und Leben bzw. gegen die sexuelle Selbstbestimmung verdächtig sind. Die jetzt gewählte Formulierung des Gesetzestextes erlaubt die Durchführung molekulargenetischer Untersuchungen auch im Fall von Straftaten von erheblicher Bedeutung, die in § 81 d Abs. 1 StPO nicht ausdrücklich genannt sind.
- § 3 Satz 3 DNA-Identitätsfeststellungsgesetz regelt, dass Auskünfte nur für Zwecke eines Strafverfahrens, der Gefahrenabwehr und der internationalen Rechtshilfe hierfür erteilt werden dürfen. Nach dem mit diesem Gesetz verfolgten Zweck hätte die *Auskunft auf Strafverfahren i. S. d. § 81 g Abs. 1 StPO beschränkt* werden müssen. Nunmehr sind Auskünfte auch für Verfahren zulässig, in deren Rahmen die Durchführung molekulargenetischer Untersuchungen nicht zulässig wäre.

Bescheidung des Antragstellers nach Verfahrenseinstellung

Im Jahresbericht 1996[122] hatten wir darüber berichtet, dass die Staatsanwaltschaft den Anzeigeerstattern, aufgrund deren Anzeige ein Ermittlungsverfahren eingeleitet wurde, in der Mitteilung über die *Einstellung des Verfahrens* nach § 154 StPO zu weit gehende Mitteilungen macht. So wurde der Tatvorwurf aus weiteren gegen den Beschuldigten laufenden Ermittlungsverfahren mitgeteilt, aus denen eine höhere Strafe zu erwarten ist, gegen die die aus dem eingestellten Ermittlungsverfahren zu erwartende Strafe nicht erheblich ins Gewicht fällt.

Die Senatsverwaltung für Justiz hat sich unserer Auffassung, dass die *Angabe des Tatvorwurfes* nicht erforderlich ist, angeschlossen und die Staatsanwaltschaften angewiesen, dem Anzeigenden Tatvorwürfe aus anderen Verfahren künftig nicht mehr mitzuteilen. Der Einstellungsbescheid gegenüber dem Anzeigenden ist zu begründen (§ 171 Satz 1 StPO), d. h., es sind die maßgeblichen tatsächlichen und rechtlichen

121 JB 1997, Anlage 2.1.2
122 4.3.1

Gründe, die zur Einstellung des Verfahrens geführt haben, anzugeben. Nr. 89 Abs. 2 Satz 1 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) sieht vor, dass die Begründung sich nicht nur auf allgemeine und nichtssagende Redewendungen beschränken darf. Demgegenüber stellt Nr. 4 a RiStBV klar, dass alles, was zu einer nicht durch den Zweck des Ermittlungsverfahrens bedingten Bloßstellung des Beschuldigten führen kann, zu vermeiden ist. Dem Interesse des Anzeigenden an einer nachvollziehbaren Begründung kann durch die Wiedergabe des Wortlautes des § 154 Abs. 1 StPO Rechnung getragen werden. Damit wird ausgesagt, dass

- die Anzeige auf ihre Auswirkungen für den Beschuldigten hin überprüft worden ist,
- gegen den Beschuldigten in einem anderen Verfahren eine Strafe oder Maßregel der Besserung und der Sicherung rechtskräftig verhängt worden oder gegen ihn ein anderes Ermittlungsverfahren anhängig ist, in dem eine solche Rechtsfolge zu erwarten ist, und
- die Strafe oder Maßregel die in dem angezeigten Verfahren zu erwartende Rechtsfolge beträchtlich übersteigt oder jedenfalls zur Einwirkung auf den Beschuldigten oder zur Verteidigung der Rechtsordnung ausreichend erscheint.

4.3.2 Finanzen

Informationszentrale für den Steuerfahndungsdienst (IZ-Steufa)

Auch in diesem Berichtsjahr wurden weder auf Bundes- noch auf Landesebene Initiativen zur Aufnahme datenschutzrechtlicher Regelungen in die *Abgabenordnung* ergriffen[123]. Die Senatsverwaltung für Finanzen hält an ihrer Auffassung fest, dass das Steuerrecht bereits umfassende, alles abdeckende Datenschutzvorschriften in Gestalt des Steuergeheimnisses enthalte[124]. Mit dieser Begründung wird nicht nur eine datenschutzrechtliche Reform der Abgabenordnung abgelehnt, sondern auch die Anwendbarkeit des Berliner Datenschutzgesetzes für die Steuerverwaltung. Diese Auffassung widerspricht den Vorgaben des Bundesverfassungsgerichtes, das unmissverständlich bereichsspezifische gesetzliche Regelungen gefordert hat. Das in der Abgabenordnung vorgesehene Steuergeheimnis erfüllt diese Voraussetzungen nicht. Das hat auch der Unterausschuss „Datenschutz“ des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin so gesehen[125] und angekündigt, eine Bundesratsinitiative Berlins zu fordern, wenn auf Bundesebene weiterhin keine Gesetzesinitiativen ergriffen werden.

123 JB 1997, 4.3.2
124 Stellungnahme des Senats zum JB 1997 zu Ziff. 4.3.2, Drs. 13/2918
125 Beschlussprotokoll des Unterausschusses „Datenschutz“ vom 12. Januar 1999, TOP 1. c

Wozu die Auffassung der Senatsverwaltung für Finanzen führt, zeigt die Vorgehensweise bei der IZ-Steufa, für die in der Abgabenordnung nur unzureichende Regelungen existieren. Die Senatsverwaltung für Finanzen weigert sich, bei der Speicherung dieser sehr sensiblen Daten die Regelungen des Berliner Datenschutzgesetzes zu beachten.

Die IZ-Steufa ist bei dem Finanzamt Wiesbaden II ansässig. Sie wurde 1977 durch eine Verwaltungsvereinbarung der alten Bundesländer ins Leben gerufen; die neuen Bundesländer sind dieser Verwaltungsvereinbarung beigetreten. Der Bundesgesetzgeber hat die IZ-Steufa 1993 durch Einführung des § 88 a AO auf eine gesetzliche Grundlage gestellt. Die IZ-Steufa hat die Aufgabe, mittels einer *Steuerstraftäter-Kartei* Auskunft über Steuerstraftäter und Tätermerkmale zu geben. Sie nimmt Informationen der mit der Steuerfahndung und sonstiger mit der Führung von Ermittlungen in Steuerstrafsachen betrauten Dienststellen der Landesfinanzbehörden entgegen, wertet sie aus und gibt diesen Dienststellen Auskunft. Die Finanzbehörden der Länder melden der IZ-Steufa Daten aus Steuerfahndungsverfahren und Steuerstrafverfahren, die dort in einer manuell geführten Datei gespeichert werden. Die Aufbewahrungsfristen hat das Hessische Ministerium der Finanzen 1993 durch einen Erlass geregelt. Die Karteikarten sind danach ohne Differenzierung zehn Jahre aufzubewahren.

Die IZ-Steufa betreibt Auftragsdatenverarbeitung für die einzelnen Bundesländer[126]. Daraus folgt, dass die Stellen des Landes Berlin, die bei der IZ-Steufa Daten verarbeiten lassen, für die Einhaltung der Vorschriften des Berliner Datenschutzgesetzes verantwortlich bleiben (§ 3 BlnDSG). Sie haben daher auch die Einhaltung des § 17 BlnDSG, der die Berichtigung, Sperrung und Löschung von Daten regelt, sicherzustellen. Danach dürfen die gemeldeten Daten bei der IZ-Steufa nur so lange gespeichert werden, wie es zur Aufgabenerfüllung der meldenden Finanzämter erforderlich ist. Die derzeitige Praxis der Berliner Steuerbehörden verstößt gegen diese Vorschrift.

Die festzulegenden *Löschungsfristen* könnten sich an § 476 Abs. 2 StPO orientieren. Dieser regelt für das Zentrale Staatsanwaltschaftliche Verfahrensregister, dass bei Einstellungen von Verfahren die Daten zwei Jahre nach der Erledigung des Verfahrens zu löschen sind, es sei denn, vor Eintritt der Löschungsfrist wird ein weiteres Verfahren zur Eintragung in das Verfahrensregister mitgeteilt. In diesem Zentralen Verfahrensregister sollen auch Daten aus Steuerfahndungs- und Steuerstrafverfahren gespeichert werden und zum Abruf der Finanzbehörden bereitstehen.

Die Finanzverwaltungen erwägen, die IZ-Steufa einzustellen, wenn das Zentrale Staatsanwaltschaftliche Verfahrensregister funktioniert. Es ist nicht ersichtlich, aus welchen Gründen eine längere Speicherung

[126] vgl. den Beschluss der 13. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28. September 1982

dieser Daten in der IZ-Steufa erforderlich ist. Jedenfalls ist die pauschale Datenspeicherung von zehn Jahren – unabhängig vom Einzelfall und vom Ausgang des Verfahrens – unverhältnismäßig.

Fahrtenbuch für Ärzte

Durch das Jahressteuergesetz 1996 wurden die ertragsteuerliche Behandlung der privaten Kfz-Nutzung sowie die Pauschalierung der privaten Pkw-Kosten vereinheitlicht. Der private Nutzungsanteil eines geschäftlich genutzten Kfz kann im Einzelfall allerdings zu einer deutlichen Steuermehrbelastung führen, denn eine Pauschalierung kann den Besonderheiten im Einzelfall nur unvollkommen Rechnung tragen. Als Ausnahme von der gesetzlich festgelegten Pauschalierung des privaten Nutzungsanteils können die auf die Privatfahrten anfallenden tatsächlichen Kosten in der Steuererklärung nur angesetzt werden, wenn die Betroffenen das Verhältnis der privaten zu den übrigen Fahrten durch ein Fahrtenbuch nachweisen. In dem Fahrtenbuch sind auch die Namen und Adressen der aufgesuchten Kunden anzugeben.

Diese nur in *Steuerrichtlinien* vorgesehene Regelung führt zu Ergebnissen, die mit dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung nicht zu vereinbaren sind. Nach dem Volkszählungsurteil des Bundesverfassungsgerichtes vom 15. Dezember 1983[127] muss für die betroffenen Kunden nachvollziehbar sein, welche Stellen welche Daten zu ihrer Person zu welchen Zwecken verarbeiten. Nach dem vom Bundesministerium der Finanzen geforderten Verfahren muss jeder Bürger damit rechnen, dass bei irgendwelchen Finanzämtern in den Anlagen zur Steuererklärung eines Dritten Daten zu seiner Person gespeichert werden. Besondere Bedeutung kommt dieser Problematik in den Fällen zu, in denen das Fahrtenbuch von zur Geheimhaltung verpflichteten Personen – wie z. B. Ärzten – geführt wird. Das Bundesministerium der Finanzen hatte deshalb 1996 entschieden, dass zumindest für Ärzte, die typischerweise Hausbesuche machen, die Angabe „Patientenbesuch“ ausreicht. Diese Entscheidung hat das Bundesministerium der Finanzen Ende 1997 aufgehoben. Seit 1998 verlangen die Finanzämter, dass Ärzte, Rechtsanwälte, Steuerberater und andere zur besonderen Geheimhaltung verpflichtete Personen zum Nachweis der beruflichen Veranlassung der Fahrt mit ihrem Wagen im Fahrtenbuch den Zweck sowie die Namen und Adressen ihrer Kunden angeben.

Die *Namen und Anschriften der aufgesuchten Patienten* unterliegen dem *Auskunftsverweigerungsrecht der Ärzte* nach § 102 Abs. 1 Nr. 3 c Abgabenordnung (AO). Bei berechtigter Auskunftsverweigerung tritt das öffentliche Interesse an der Sachaufklärung insoweit zurück, und dem Schutz des jeweils in Frage stehenden Vertrauensverhältnisses

[127] BVerfGE 65,1, 46

wird Vorrang eingeräumt[128]. Nach § 102 Abs. 1 Nr. 3 c AO können Ärzte über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekannt geworden ist, gegenüber den Finanzbehörden die Auskunft verweigern. Ob der Arzt hiervon Gebrauch macht, muss seiner freien Entscheidung überlassen bleiben. Soweit Ärzte gezwungen sind, zur Wahrung steuerlicher Interessen ein Fahrtenbuch zu führen, stellt die Forderung nach der Angabe von Namen und Anschriften ihrer Patienten eine unzulässige Verpflichtung dar. Die Patienten haben darüber hinaus ein durch § 203 Strafgesetzbuch (StGB) geschütztes Interesse an der Verschwiegenheit des Fahrtenbuchführenden. Dieses Interesse bezieht sich nicht nur auf den Inhalt des im Rahmen des Besuches geführten Gespräches, sondern kann bereits durch die Offenbarung der Tatsache, dass ein Besuch stattgefunden hat, verletzt werden[129]. Nach § 203 Abs. 1 Nr. 1 StGB macht sich ein Arzt strafbar, der unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm in seiner Eigenschaft als Arzt anvertraut oder sonst bekannt geworden ist.

Haushaltsplan als Adressbuch

Der Haushaltsplan 1998 versetzte Mitarbeiter und Behördenleitung einer Berliner Behörde in Erstaunen – mussten sie doch feststellen, dass er bei den Einnahmen der Behörde die genauen Anschriften der Dienstwohnungen der Mitarbeiter einschließlich der zu zahlenden Jahresmiete auflistete.

Der Haushaltsplan dient der Feststellung und Deckung des Finanzbedarfes, der zur Erfüllung der Aufgaben Berlins im Bewilligungszeitraum voraussichtlich notwendig ist; er ist Grundlage für die Haushalts- und Wirtschaftsführung (§ 1 Landeshaushaltsordnung (LHO)). Zur Erstellung des Haushaltsplanes haben die öffentlichen Stellen beizutragen, indem sie der Senatsverwaltung für Finanzen eine Aufstellung über ihre zu erwartenden Einnahmen und Ausgaben zur Verfügung stellen. Die Senatsverwaltung für Finanzen hatte im Aufstellungs-Rundschreiben 1998 dazu aufgefordert, in dem Titel „Mieten für Grundstücke, Gebäude und Räume“ der betroffenen Behörde die vermieteten, verpachteten oder sonstigen zur Nutzung überlassenen Objekte einzeln unter Angabe der Lage (regelmäßig Straße und Hausnummer), der Fläche, der monatlichen Miete/Pacht je Quadratmeter sowie der erwarteten Einnahmen aufzuführen. Diese Daten sind dann von der Senatsverwaltung für Finanzen in den Haushaltsplan übernommen und veröffentlicht worden.

128 BVerfG, NJW 1990, 701
129 BGHSt 33, 148 (151) zu § 53 Abs. 1 Nr. 3 StPO

Die Veröffentlichung der detaillierten *Angaben zu den Vertragsverhältnissen* stellt eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches dar (§ 13 BlnDSG), da der Haushaltsplan öffentlich ausliegt, z. B. in allen Bezirksämtern und in den Stadtbibliotheken. Das ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Es handelt sich hier um personenbezogene Daten, da bei genauer Bezeichnung des Objektes und Angabe des Mietzinses nachvollziehbar war, welcher Mieter welcher Wohnung welchen Mietpreis entrichtete. Da weder eine Einwilligung der betroffenen Mieter vorlag noch die LHO die Veröffentlichung erlaubt, war sie unzulässig.

Die Senatsverwaltung für Finanzen hat inzwischen in dem Aufstellungs-Rundschreiben 1999 klargestellt, dass der Schutz personenbezogener Daten Vorrang vor der Transparenz des Haushaltsplanes hat.

4.4 Sozialordnung

4.4.1 Arbeitnehmer und öffentliche Bedienstete

Routineabfragen bei der SCHUFA als Präventivmaßnahme „psychologischer Natur“

Durch Zufall erfuhr ein Mitarbeiter eines bekannten Unternehmens, dass sein Arbeitgeber Auskünfte bei der SCHUFA GmbH eingeholt hatte. Darüber hinaus stellte sich in der Folgezeit heraus, dass solche Anfragen bei allen Arbeitnehmern einer bestimmten Filiale durchgeführt wurden und dies im Übrigen auch in allen Arbeitsverträgen (außer dem des Petenten) so geregelt war. Diese Vorgehensweise wurde vom Unternehmen damit begründet, dass es in dieser Filiale in der Vergangenheit zu erheblichen Diebstählen gekommen sei und diese Maßnahme insoweit eine „reine Präventivmaßnahme psychologischer Natur vor dem Hintergrund der Eigentumssicherung innerhalb des Unternehmens“ darstelle. Im Übrigen würden SCHUFA-Auskünfte grundsätzlich unter Einbindung des/der Betroffenen erfolgen, die vorliegend reklamierte Angelegenheit sei ein bedauerlicher Einzelfall.

Nach dem Vertrag zwischen der Schutzgemeinschaft für allgemeine Kreditsicherung GmbH (SCHUFA) und den am Verfahren beteiligten Unternehmen und Banken dürfen Einzelhandelsunternehmen ausschließlich bei Konsumentenkrediten Auskünfte bei der SCHUFA einholen, nicht dagegen zur Überwachung von Mitarbeitern (1.3.2 des Vertrages zur technischen Abwicklung des SCHUFA-Verfahrens). Die beim Arbeitsverhältnis durch Gesetz oder von der Rechtsprechung etwa im Zusammenhang mit dem *Fragerecht des Arbeitgebers* entwickelten Informationssperren sind auch nicht mit einer Einwilligung des Arbeitnehmers zu überwinden. Dies kann auch nicht durch eine Selbstauskunft des Arbeitnehmers umgangen werden.

Das Unternehmen hat mitgeteilt, die in den Arbeitsverträgen bisher obligatorischen Passagen zu SCHUFA-Auskünften nicht mehr zu verwenden und diese auch in den Altverträgen zu streichen.

Ein ehemaliger Mitarbeiter eines großen Unternehmens benötigte zur Vorbereitung und zur Vervollständigung seiner Unterlagen für seinen Antrag auf Altersrente eine Aufstellung über die Brutto-Jahresgehaltssummen für einen zurückliegenden Zeitraum von ca. 20 Jahren. Der Petent stützte sein Begehren auf § 18 c Abs. 2 Sozialgesetzbuch IV (SGB IV), wonach ein gesetzlicher Anspruch auf eine solche Bescheinigung über das tatsächliche Arbeitseinkommen unabhängig davon besteht, ob die BfA diese Summen aktuell zur Rentenberechnung benötigt oder nicht. Soweit dies nicht gilt, bestehe zumindest der allgemeine Auskunftsanspruch (§ 34 BDSG). Das Unternehmen wies den Wunsch des Petenten mit der Begründung zurück, die angeführten gesetzlichen Regelungen könnten hier nicht angewendet werden, da sich diese Bestimmungen nur auf das letzte Kalenderjahr und § 34 Abs. 1 BDSG sich nur auf EDV-mäßig gespeicherte Daten beziehe.

Der sozialrechtliche Anspruch ist tatsächlich auf das letzte Kalenderjahr begrenzt. Ein Auskunftsrecht ergibt sich aber sowohl aus dem Bundesdatenschutzgesetz als auch aus dem Betriebsverfassungsgesetz (BetrVG). Nach § 34 Abs. 1 BDSG kann der Betroffene Auskunft verlangen über die zu seiner Person gespeicherten Daten. Zwar gilt das Bundesdatenschutzgesetz nur für personenbezogene Daten in oder aus Dateien und nicht für Akten. Nach § 27 Abs. 2 BDSG kommt diese Vorschrift in diesem Fall dennoch zur Anwendung, da der Petent geltend macht, die gewünschten Daten lägen heute zwar nicht mehr automatisiert vor, jedoch wisse er aus seiner Zeit als ehemaliger EDV-Projektant, dass dies früher der Fall gewesen sei. Ein Anspruch auf *Einsichtnahme* besteht auch nach § 83 BetrVG. Auch ausgeschiedenen Mitarbeitern steht das personalaktenrechtliche Einsichtsrecht zu; dies begründet als Minus auch einen Auskunftsanspruch.

Auch eine Entscheidung des Arbeitsgerichts Kaiserslautern zur *Erteilung von Lohnbescheinigungen* kann hier übertragen werden. Danach folgt die Pflicht des Arbeitgebers, dem Arbeitnehmer eine besondere Bescheinigung über die Höhe seines Lohnes auszustellen, aus der allgemeinen, aus § 242 BGB abzuleitenden Fürsorgepflicht des Arbeitgebers. Der Arbeitnehmer muss lediglich darlegen, dass er zu einem bestimmten Zweck eine bestimmte Lohnbescheinigung benötigt, z. B. für die Erlangung eines Bankkredits. Bei Vorliegen des berechtigten Interesses ist der Arbeitgeber auch dann zur Erteilung besonderer Lohnbescheinigung verpflichtet, wenn dies zu verwaltungsmäßigem Mehraufwand gegenüber EDV-erstellten Lohnabrechnungen führt[130].

Das Unternehmen hat dem Petenten schließlich die gewünschte Auskunft erteilt.

130 ARSt 1988, S. 146

Personaldaten und Verwaltungsreform

„Keine Verwaltungsreform ohne Datenzugriff" – so hatten wir im vergangenen Jahr unsere Abhandlung zur *DV-gestützten Kosten- und Leistungsrechnung* in der Berliner Verwaltung überschrieben[131]. In diesem Jahr mussten wir feststellen, dass das hierfür eingesetzte Verfahren eine Fehlfunktion enthielt, die den unkontrollierten Zugriff auf sensible Mitarbeiterdaten durch unberechtigte Dritte ermöglichte.

Die in der Einführung befindliche Kosten- und Leistungsrechnung soll dazu dienen, Transparenz über die Kosten des Verwaltungshandelns zu gewinnen. In diesem von der Software *ProFISKAL* im Rahmen der Neukonzeption des automatisierten Haushaltswesens unterstützten Verfahren werden daher auch personenbezogene Daten der Beschäftigten verarbeitet, um die jeweiligen Personalkostenanteile an den einzelnen Verwaltungsleistungen ermitteln zu können[132]. Bei diesen Daten handelt es sich sowohl um „Stammdaten", die unter anderem die Eingruppierungssätze der einzelnen Beschäftigten umfassen, als auch um „Bewegungsdaten", die sich aus der laufenden Arbeit als Buchungssätze ergeben.

Das Einrichten und die Pflege der Personalstammdaten sowie das Buchen von Bewegungsdaten aus der Zeitstatistik werden von eigens dafür geschulten „Sachbearbeitern Kostenrechnung" für deren jeweiligen Zuständigkeitsbereich wahrgenommen. Systemseitig ist hierfür eine Zugriffsbeschränkung der Anwender vorgesehen, die auf einer Zuordnung der Nutzerrechte auf „Ident-Gruppen" basiert. Den Sachbearbeitern Kostenrechnung soll der Datenzugriff hierdurch nur für den Bereich ihrer Kostenstelle ermöglicht sein. Die Struktur der Kostenstellen folgt dabei zumeist der bezirklichen Ämterstruktur.

Diese *Zugriffsbeschränkung* gilt lediglich im Fall der Bewegungsdaten. Der Zugriff auf die Personalstammdaten – und damit auf die Eingruppierungsdaten der Beschäftigten – war den Sachbearbeitern Kostenrechnung jedoch kostenstellenübergreifend für den Bereich des gesamten Bezirksamtes möglich. Um diese programmseitige Fehlfunktion der Nutzerberechtigung auszulösen, bedurfte es lediglich eines Vertippens bei der Eingabe der Kostenstellennummer, der gezielten Eingabe einer organisationsfremden Nummer oder des Einsatzes eines |*| als „Joker" bei der Suche; letzteres stellt bei der Arbeit unter ProFISKAL eine gebräuchliche Funktion dar, die auch in den einschlägigen Schulungen vermittelt wird.

Durch diese Fehlfunktion hatten die „Sachbearbeiter Kostenrechnung" ämterübergreifend einen lesenden und schreibenden Zugriff auf sämtliche Eingruppierungsdaten aller Beschäftigten des jeweiligen

131 JB 1997, 4.4.1
132 vgl. auch: JB 1995, 3.6

Bezirksamtes. Eine Zuordnung der Eingruppierungen auf die jeweiligen Mitarbeiter ist dabei aus so genannten „Identen“ ersichtlich. Als Identifikationsmerkmal wurden überwiegend die Stellenzeichen, teils gar unmittelbar die Namen der Beschäftigten gewählt. Wäre – wie ursprünglich in einzelnen Bezirksverwaltungen geplant – tatsächlich die Personalnummer als Ident zum Einsatz gelangt[133], wäre dieser Schlüssel zu sämtlichen Personaldaten der jeweiligen Mitarbeiterinnen und Mitarbeiter durch den beschriebenen Programmfehler in unzulässiger Weise und unkontrolliert dem potentiellen Zugriff sämtlicher – also auch der organisationsfremden – Sachbearbeiter Kostenrechnung ausgesetzt gewesen.

Recherchen bei der Senatsverwaltung für Finanzen, die für die Einführung der KLR-Software verantwortlich ist, ergaben, dass diese Fehlfunktion auch anhand der Testdatenbank nachvollziehbar war und dass der beschriebene *Programmfehler* mindestens seit Mitte August 1997 bekannt war. Gleichwohl wurde das Programm anschließend in weiteren Verwaltungen, u. a. auch bei der Senatsverwaltung für Finanzen selbst, eingesetzt.

Eingruppierungsdaten der Beschäftigten gehören zu den besonders geschützten Personalaktendaten i. S. d. §§ 56 ff. Landesbeamtengesetz (LBG), die analog auch auf Angestellte und Lohnempfänger anzuwenden sind. Diese Daten sind nach § 56 Abs. 1 Satz 1 LBG vor unbefugter Einsicht zu schützen. Bei der automatisierten Verarbeitung personenbezogener Daten ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (§ 5 Abs. 3 Nr. 5 BlnDSG).

Künftig ist eine Überprüfung der Zugriffsberechtigungen in die Prüfkonzepte aufzunehmen, soweit mit entsprechenden Programmen personenbezogene Daten verarbeitet werden.

Mitte Oktober 1998 wurde die überarbeitete Programmversion von ProFISKAL den Bezirken zur Verfügung gestellt; in dieser Programmversion tritt der beschriebene Fehler nicht mehr auf.

4.4.2 Gesundheit

Medizinische Daten

Ein Frauenarzt lud mit offener Postkarte seine Patientin zur „Weiterbehandlung im Laufe der nächsten Woche zur Krebsvorsorgekontrolle“ in seine Sprechstunde ein. Der Zufall wollte, dass die Nachricht im falschen Briefkasten landete. Wiederholt wurde von Patienten auch auf offen ausliegende Patientenkarteikarten auf dem Tresen des ärztlichen Empfangsraumes hingewiesen.

[133] vgl. JB 1997, 4.4.1

Der Vorfall sowie andere Nachlässigkeiten im Praxisbetrieb niedergelassener Ärzte veranlassten uns, bei der Ärztekammer anzuregen, dass sie im Rahmen ihrer Aufgaben Ärzte verstärkt auf die Wahrung der ärztlichen Schweigepflicht auch beim *alltäglichen Praxisbetrieb* hinweist. Die Ärztekammer hat daraufhin nicht nur einen Beitrag zum Datenschutz in ihrer Verbandszeitschrift „Berliner Ärzte“ veröffentlicht, um „praxisblinde“ Berufskollegen auf die Bedeutung des Vertrauensverhältnisses mit den Patienten hinzuweisen. Sie hat auch die Zusage gegeben, etwaigen Verstößen gegen die Schweigepflicht der Ärztlichen Berufsordnung mit allen ihr zu Gebote stehenden Mitteln entgegenzutreten.

Ein Gesundheitsamt befindet sich im oberen Teil eines Hochhauses, der durch Fahrstuhl und Treppenhaus zu erreichen ist. Der an das Treppenhaus und den Fahrstuhl angrenzende Flurbereich ist zugleich Warteraum und Archiv für die Krankengeschichten und sonstigen Patientenunterlagen. Bei einer der Überprüfung konnten wir ungestört über einen langen Zeitraum hinweg aus den leicht zu öffnenden Hängeordnern beliebig viele Patientenakten herausnehmen und durchblättern, bis schließlich eine Mitarbeiterin hierauf aufmerksam wurde.

Eine unangekündigte Prüfung bestätigte, dass die Mängel unverzüglich beseitigt wurden. Der Erfolg dieser Überprüfung war so groß, dass das Gesundheitsamt wenig später in seinen neu bezogenen Diensträumen um eine weitere datenschutzrechtliche Überprüfung bat, um nun vom Amt selbst erkannte datenschutzrechtliche Mängel bei der *Gestaltung der Räume* und der *Aktenverwahrung* besser beheben zu können.

Krankenhaus oder Bahnhofshalle

Die Patienten eines Krankenhauses wunderten sich nicht schlecht, als in ihren Krankenzimmern und in den Warteräumen aus einer zentralen Lautsprecheranlage Aufrufe ertönten wie: „Herr Schmidt, Herr Müller, Herr Meier und Frau Schulze, bitte nach vorne kommen“ oder „Herr Schmidt, Herr Müller, Herr Meier und Frau Schulze, bitte zum Ultraschall nach vorne kommen“, oder „Frau Müller und Frau Schmidt, bitte zum Verbandswechsel erscheinen!“. Umso schockierter waren sie, als diese Ausrufe sich nicht nur auf ihr eigenes Krankenzimmer bzw. Wartezimmer beschränkten, sondern zumindest auf der ganzen Etage zu hören waren.

Da nach dem Landeskrankenhausgesetz das Krankenhaus zu gewährleisten hat, dass auf Patientendaten nur zugegriffen werden darf, soweit dies für die Behandlung erforderlich ist, lag ein Verstoß gegen diese Vorschrift und auch gegen die ärztliche Schweigepflicht vor.

Die Krankenhausleitung hat durch Dienstanweisung angeordnet, dass *Patientenaufrufe per Lautsprecherdurchsage* in den Krankenzimmern zu unterbleiben haben und die Rufanlage nur noch als Personal-

aufruf in Notfallsituationen benutzt werden darf. Die erforderlichen Aufrufe an Patienten für Behandlungsmaßnahmen wurden durch andere Verfahren ersetzt.

Ein Stadtrat auf Therapietripp

Eine ganz besondere Verantwortung übernahmen der Stadtrat für Gesundheit und Soziales eines Berliner Bezirkes und eine Justitiarin, als sie entschieden, sich praktische Erfahrungen bei der Suchttherapie zu verschaffen. Sie beschlossen, als Hospitanten an einer Therapie teilzunehmen. In einem Berliner Krankenhaus wurde unter ärztlicher Leitung eine Suchttherapie insbesondere für Alkoholiker angeboten und durchgeführt. Seit Jahren wurden hierzu als „Hospitanten" Mitarbeiter aus Bezirksämtern zugelassen, die sich mit der Suchtproblematik vertraut machen wollten. Ein Patient verabschiedete sich entsetzt aus der Therapie, als er den Leiter seiner Behörde und die Justitiarin in seiner Therapiegruppe erkannte.

Sämtliche Begleitumstände einer ärztlichen Behandlung, die zur Identifizierung eines Patienten führen könnten, sind von der ärztlichen Schweigepflicht mit umfasst. Nur wenn der Patient zuvor über die Identität des Hospitanten genauestens informiert worden ist und dann seine ausdrückliche Einwilligung erteilt hat, könnte an eine *Gastteilnahme bei Therapiesitzungen* gedacht werden. Es ist jedoch davon auszugehen, dass dies einen erheblichen Aufwand erfordert. Denn es reicht nicht aus, dass der Patient sein Einverständnis erklärt, „irgendein" Hospitant könne an seinem Arzt-Patienten-Gespräch teilnehmen. Gerade der vorliegende Fall zeigt, dass es zu äußerst unangenehmen Überraschungen kommen könnte. Der Hospitant muss also zuvor dem Patienten gegenüber benannt werden, damit dieser in der Lage ist, die Entscheidung zu fällen, ob er mit dessen Gegenwart einverstanden ist oder nicht. Bei dem vorliegenden Fall handelte es sich um eine Gruppenveranstaltung von etwa 35 bis 40 Teilnehmern, die alle zuvor ihr Einverständnis hätten erklären müssen. Da alldies nicht geschehen war, war diese Art von Veranstaltung ein grober Verstoß gegen die ärztliche Verschwiegenheitspflicht. Die Senatsverwaltung für Gesundheit hat die Krankenhäuser angewiesen, das Vertrauen der Patienten in die ärztliche Schweigepflicht nicht mehr in dieser Weise zu hintergehen.

Eine altersschwache Einwilligungserklärung

Ein schwer behinderter Patient hatte 1989 dem Landesversorgungsamt eine Entbindungserklärung von der ärztlichen Schweigepflicht abgegeben, die dort zu den Akten genommen worden war. Der Patient verzog in ein anderes Bundesland. Das Versorgungsamt Berlin forderte bei einer Behörde des anderen Bundeslandes ärztliche Befundberichte über den Petenten an und erhielt sie. Das Versorgungsamt stützte sich auf die alte Schweigepflicht-Entbindungserklärung. Die Anerkennung des Petenten als Schwerbehinderter in dem damaligen Verfahren war jedoch bereits 1989 abgeschlossen. Weitere Anträge waren von dem Petenten zwischenzeitlich beim Versorgungsamt nicht gestellt worden. Eine aktuellere Schweigepflicht-Entbindungserklärung lag nicht vor.

Das Versorgungsamt war der Annahme, eine Erklärung über die *Entbindung von der ärztlichen Schweigepflicht* gelte, sofern eine Nachuntersuchung von Amts wegen vorgesehen ist, über den eigentlichen Abschluss des Verfahrens hinaus. Dem ist nicht so. Vielmehr endet die Entbindung von der ärztlichen Schweigepflicht mit dem Abschluss des Feststellungsverfahrens. Für weitere Verfahrensschritte ist eine neue Entbindung von der ärztlichen Schweigepflicht einzuholen.

Der große Bluff

Eine Patientin, die sich einer Gelenkoperation unterziehen musste, wurde zum Medizinischen Dienst bestellt. Dort verordnete die Ärztin eine verlängerte Krankschreibung. Nach dem Ablauf der Krankschreibung wurde die Patientin vom stellvertretenden Verwaltungsdirektor ihres Arbeitgebers mit der Bemerkung angesprochen, dass er von der Krankenkasse um Auskunft darüber gebeten worden sei, ob ihre Fehlzeiten wegen der Fußoperation berechtigt gewesen wären. Die erregte Patientin bat uns um Prüfung, ob es zulässig sei, dass ein medizinisch nicht qualifizierter Vorgesetzter für die Kasse Entscheidungen des Medizinischen Dienstes kontrolliere.

Die Überprüfung bei der AOK ergab, dass mitnichten von dort ein solches Ansinnen an den Arbeitgeber gerichtet worden war. Vom Medizinischen Dienst waren schon gar nicht solche Fragen an den Arbeitgeber gerichtet worden. Der Arbeitgeber hatte somit die Anfrage der AOK frei erfunden, um die Petentin unter Druck zu setzen.

Approbation und Patientenschutz

Am 1. Januar 1999 ist das *Psychotherapeutengesetz* (PsychThG) in Kraft getreten[134]. Das Gesetz regelt die Ausbildung und Berufsausübung von Psychotherapeuten mit einem Abschluss im Studiengang Psychologie bzw. Pädagogik/Sozialpädagogik.

Wer ab 1. Januar 1999 heilkundliche Psychotherapie unter der Berufsbezeichnung Psychologische/r Therapeut/in bzw. Kinder- und Jugendlichenpsychotherapeut/in ausüben will, benötigt hierfür eine *Approbation*. Hierfür müssen vom Antragsteller Nachweise über geleistete Behandlungsstunden erbracht werden. In § 12 Abs. 3 und 4 PsychThG wird von dokumentierten Behandlungsfällen gesprochen. Das ist

[134] Gesetz über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichenpsychotherapeuten, zur Änderung des Fünften Buches Sozialgesetzbuch und anderer Gesetze vom 16. 6. 1998, BGBl. I vom 23. 6. 1998, S. 1311 (1315)

jedoch keine gesetzliche Ermächtigung zur Übermittlung von Patientendaten an die Approbationsbehörde. Die Datenschutzbeauftragten sind deshalb der Meinung, dass der Nachweis in anonymisierter Form zu führen ist. Die Senatsverwaltung für Gesundheit und Soziales hat ein Verfahren gewählt, welches die Anonymität der Patienten nicht gefährdet und der Nachweis gegenüber der Behörde gleichwohl in Form von Abrechnungsbelegen oder nötigenfalls durch anonymisierte Falldarstellungen möglich ist.

4.4.3 Sozialverwaltung

„Sozialamtsfalle" legitimiert

Nahezu seit In-Kraft-Treten des Zehnten Buches des Sozialgesetzbuches (SGB X) im Jahr 1981 war umstritten, wie die Bestimmung des § 68 SGB X auszulegen sei, die alle Sozialleistungsträger berechtigt, ohne weitere inhaltliche Voraussetzungen bestimmte Daten an die Polizei- und andere Sicherheitsbehörden herauszugeben: Neben Name, Vorname, Geburtsdatum des Betroffenen sowie Namen und Anschriften seiner derzeitigen Arbeitgeber durfte seine „derzeitige Anschrift" herausgegeben werden. Die Weitergabe darüber hinausgehender Daten setzte eine richterliche Anordnung voraus (§ 73 Abs. 3 SGB X), wenn es sich nicht um Straftaten im Zusammenhang mit der Gewährung der Sozialleistung (z. B. Sozialleistungsmissbrauch) handelte (§ 69 Abs. 1 Ziff. 1 SGB X).

Obwohl niemand einen vernünftigen Zweifel daran haben konnte, was „derzeitige Anschrift" eines Sozialleistungsempfängers bedeutet, nämlich seinen Wohnsitz oder jedenfalls einen Ort, „wo er sich unter Umständen aufhält, die erkennen lassen, dass er an diesem Ort oder in diesem Gebiet nicht nur vorübergehend verweilt" („gewöhnlicher Aufenthalt", § 30 Abs. 3 S. 2 SGB I), drängten die Sicherheitsbehörden von jeher darauf, dass auch der *momentane Aufenthalt* – etwa in einer Sozialbehörde zwecks Beratung – als derzeitige Anschrift zu verstehen sei.

> *Ein ausländischer Arbeitsloser war zur Haft ausgeschrieben, weil er seiner Ehefrau in einer Auseinandersetzung die Handtasche weggenommen hatte. Als er wieder einmal im Arbeitsamt erschien, informierte eine Sachbearbeiterin die Polizei. Als deren Vorgesetzter hiervon hörte, schickte er den Betroffenen weg. Dies trug ihm eine Strafanzeige wegen Strafvereitelung im Amt ein.*

Anhand dieser eigenwilligen Fallkonstellation entschied das Berliner Kammergericht, das nur für strafrechtliche, nicht aber für sozialrechtliche Fragestellungen zuständig ist, im Jahr 1983, dass „der Begriff der derzeitigen Anschrift gewissermaßen als Minus auch den gegenwärtigen Aufenthalt" umfasse[135]. Diese kaum nachvollziehbare und in der Literatur einhellig abgelehnte Einscheidung führte zu einer unterschiedlichen Praxis bei Bund und Ländern und bei den verschiedenen Sozialbehörden. Auch in Berlin weigerte sich ein Teil der Sozialbehörden standhaft, ohne richterliche Anordnung das Erscheinen von Leistungsempfängern im Amt noch während deren Anwesenheit der Polizei anzuzeigen.

Diese wiederum begnügte sich nicht mehr mit der Forderung nach Mitteilung des momentanen Aufenthalts, vielmehr verlangte man zunehmend von Sozialbehörden auch eine Information über den *nächsten Vorsprachetermin,* also den künftigen Aufenthalt – mit dem Argument, dieser sei ebenfalls unter den Begriff „derzeitige Anschrift" zu subsumieren: Den Sozialverwaltungen wurde also zugemutet, ihren Hilfeempfängern eine Falle zu stellen, damit die Polizei die Ahnungslosen bequem verhaften kann.

Die Senatsverwaltung für Gesundheit und Soziales, die zuvor in einem Gemeinsamen Rundschreiben von 1984 noch die Auffassung vertreten hatte, nach § 68 SGB X dürfte (entsprechend § 30 Abs. 3 SGB I) nur der tatsächliche Aufenthalt von längerer Dauer, also nicht der kurzfristige Aufenthalt in einer Behörde eines Sozialleistungsträgers, mitgeteilt werden, gab dem Druck nach und verfasste gemeinsam mit den Senatsverwaltungen für Schule, Jugend und Sport sowie für Inneres ein Rundschreiben, nach dem – allerdings eingeschränkt auf Fälle eines Untersuchungs-, Vollstreckungs- oder Sicherungshaftbefehls sowie eines Unterbringungsbefehls – der „momentane oder wiederkehrende Aufenthalt in der Dienststelle eines Sozialleistungsträgers" mitzuteilen ist[136].

Der Schwierigkeiten mit der eigenwilligen Deutung des Begriffs der „derzeitigen Anschrift" bewusst, hatte die Senatsverwaltung schon zuvor den Versuch unternommen, durch Bundesratsinitiativen eine Änderung des § 68 SGB X zu erreichen – ergebnislos. Erst im vergangenen Jahr gelang es, versteckt in einer völlig unverfänglichen Materie, nämlich dem Medizinproduktegesetz[137], diese Bestimmung dahingehend zu ergänzen, dass auch der „derzeitige oder zukünftige Aufenthaltsort" mitgeteilt werden darf – allerdings nur im „Einzelfall auf Ersuchen". Pauschale Übermittlungsersuchen etwa hinsichtlich aller Personen, die zur Fahndung ausgeschrieben sind, scheiden damit aus. Ob diese Bestimmung, die letztlich die staatliche Fallenstellerei legalisiert, Bestand haben kann, muss sich zeigen.

Das Rundschreiben zu § 68 SGB X wurde, aufgrund der gesetzlichen Vorgabe eingeengt auf Fälle des Ersuchens im Einzelfall, schließlich im Januar 1999 vom Senat als Allgemeine Anweisung, mithin als alle Bezirke bindende Vorschrift, beschlossen.

135 KG Berlin, Urteil vom 26. 5. 1983, (3) Ss 314/82 (10/83)

136 Dienstblatt Teil IV Nr. 2 v. 9. 5. 97, S. 21 f.

137 vgl. 1.1

Erheblich schärfere öffentliche Debatten hat das Unterfangen ausgelöst, die Sozialbehörden auch zur Übermittlung von Daten über den derzeitigen und künftigen Aufenthalt ausländischer Leistungsempfänger, die über keine gültige Aufenthaltsgenehmigung oder Duldung verfügen oder die eine räumliche Beschränkung missachten, an die Ausländerbehörden zu verpflichten. Ursprünglich hatte die Senatsverwaltung für Inneres gefordert, entsprechende Bestimmungen auch in das Rundschreiben zu § 68 SGB X aufzunehmen. Wegen der Abstimmungsschwierigkeiten unterblieb dies jedoch, vielmehr verfassten die beteiligten Senatsverwaltungen ein eigenes Rundschreiben[138], das bald darauf vom Senat als Allgemeine Anweisung[139] beschlossen wurde, um dem heftigen Widerstand einiger Sozialämter entgegenzuwirken.

Zwar enthält § 71 Abs. 2 SGB X besondere Offenbarungsbefugnisse für die *Übermittlung von Sozialdaten an die Ausländerbehörde.* Danach ist eine Übermittlung von Sozialdaten eines Ausländers zulässig, soweit sie erforderlich ist für die Erfüllung der in § 76 Abs. 2 des Ausländergesetzes bezeichneten Mitteilungspflichten (§ 71 Abs. 2 Satz 1 Ziff. 2 SGB X). Nach dieser Bestimmung haben zwar alle Behörden die zuständige Ausländerbehörde zu unterrichten, wenn sie Kenntnis erlangen von dem „Aufenthalt eines Ausländers, der weder eine erforderliche Aufenthaltsgenehmigung noch eine Duldung besitzt". Der Haken bei der Sache ist aber, dass diese Bestimmung nichts darüber sagt, welche Daten im Einzelnen zu übermitteln sind; der Entwurf einer bundeseinheitlichen allgemeinen Verwaltungsvorschrift, die eine entsprechende Präzisierung vornehmen soll, wird seit Jahren beraten, ist aber auch im vergangen Jahr nicht verabschiedet worden. So bleibt nichts anderes, als nach dem Wortsinn vorzugehen: „Aufenthalt" im ausländerrechtlichen Sinne meint die Tatsache, dass sich eine Person im Bundesgebiet aufhält (daher „Aufenthaltsgenehmigung"), nicht aber, wo sich die Person gerade oder künftig im Einzelnen befindet. Somit beschränkt sich die Offenbarungsbefugnis nach § 76 Abs. 2 darauf, dass sich der Betroffene in Deutschland befindet.

Sollen weitere Daten, wie z. B. über den derzeitigen oder künftigen Aufenthalt, übermittelt werden, müssen also auch die Ausländerbehörden auf die allgemeinen Offenbarungsbefugnisse des SGB X zurückgreifen. Da Ausländerbehörden als „Behörden der Gefahrenabwehr" zu betrachten sind, stehen ihnen dabei die Befugnisse des § 68 SGB X zur Verfügung, also nach der neuen Rechtslage auch das Recht, Daten über den derzeitigen und künftigen Aufenthalt zu erfahren. Dies gilt allerdings auch hier nur „im Einzelfall auf Ersuchen". Soll eine Falle gestellt werden, ist dies nur in einem zweistufigen Verfahren möglich:

138 Rundschreiben über die Übermittlung von Sozialdaten an die Berliner Ausländerbehörde gem. § 71 Abs. 2 SGB X i.V.m. § 76 Abs. 2 Ausländergesetz vom 2. Januar 1997 – Dienstblatt Teil IV, S. 19 ff.

139 Allgemeine Anweisung über die Übermittlung von Sozialdaten an die Berliner Ausländerbehörde gem. § 71 Abs. 2 SGB X i.V.m. § 76 Abs. 2 Ausländergesetz vom 13. Mai 1997

Erscheint ein Ausländer ohne Aufenthaltsgenehmigung oder Duldung in einer Sozialbehörde, unterrichtet diese die Ausländerbehörde über die Tatsache, dass dieser sich in Deutschland befindet. Die Ausländerbehörde ihrerseits überprüft dann, ob weitere Informationen erforderlich sind, z. B. um den Ausländer abschieben zu können. Ist dies aufgrund der rechtlichen und tatsächlichen Umstände der Fall, richtet die Ausländerbehörde ein Ersuchen nach § 68 SGB X an die Sozialbehörde, die nunmehr den künftigen Aufenthalt mitteilen kann – wenn nicht andere Gründe dagegensprechen. So ist eine Übermittlung auch nach § 68 SGB X unzulässig, wenn Grund zur Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Wir haben, auch unterstützt vom Unterausschuss Datenschutz des Innenausschusses des Abgeordnetenhauses, vorgeschlagen, die bisherige, unserer Auffassung nach mit der Rechtslage nicht übereinstimmende Allgemeine Anweisung durch Einführung dieses zweistufigen Verfahrens gesetzeskonform auszugestalten. Dies hat die Senatsverwaltung für Inneres abgelehnt, was allerdings an der Rechtslage nichts ändert: Soll von einer Sozialbehörde über die Mitteilung des Aufenthalts im Bundesgebiet hinaus auch der derzeitige oder künftige Aufenthalt mitgeteilt werden, ist dies nur auf der Grundlage der Allgemeinen Anweisung zu § 68 SGB X in der ab Januar 1999 gültigen Form zulässig.

Die Rasterung kommt in Fahrt – der Erfolg ist ungewiss

Seit einiger Zeit wird die Abrasterung der Daten der Sozialbehörden untereinander, aber auch ihrer Daten mit anderen Behörden als Allheilmittel gegen den angeblich allgegenwärtigen Missbrauch von Sozialleistungen propagiert; der Bundesgesetzgeber hatte für den Bereich der Sozialhilfe mit einer inzwischen schon wieder „nachgebesserten" Neufassung des § 117 Bundessozialhilfegesetz (BSHG) die erforderlichen Rechtsgrundlagen geschaffen. Danach können Sozialämter im Wege eines *automatisierten Datenabgleichs* bundesweit ihre Daten mit der Bundesanstalt für Arbeit, den Unfall- und Rentenversicherungsträgern (Abs. 1), allen anderen Sozialhilfeträgern (Abs. 2) sowie innerhalb der Verwaltung des Sozialleistungsträgers mit anderen Stellen der Verwaltung und wirtschaftlichen Unternehmen (Abs. 3) abgleichen. Übermittelt werden können nach letzterer Vorschrift außer den Personalien Daten über die Wohnung, über Verbrauchswerte und über die Eigenschaft als Kraftfahrzeughalter.

Für das Verfahren nach § 117 Abs. 1, 2 BSHG ist inzwischen die erforderliche Rechtsverordnung in Kraft[140], das Berliner Ausführungsgesetz zum BSHG (AGBSHG) wurde entsprechend angepasst[141], die Konkreti-

140 Sozialhilfedatenabgleichsverordnung – SozhiDAV v. 21. 1. 98, BGBl. I, 103 ff.

141 Gesetz zur Ausführung des Asylbewerberleistungsgesetzes und zur Änderung des Gesetzes zur Ausführung des Bundessozialhilfegesetzes, Art. II: Änderung des Gesetzes zur Ausführung des Bundessozialhilfegesetzes vom 10. Juni 1998, GVBl. S. 129 f.

sierung in einer Rechtsverordnung auf Landesebene steht allerdings noch aus. Die bundesweite technische Umsetzung, bei der die Rechenstelle der Rentenversicherungsträger in Würzburg eine zentrale Rolle spielt, ist erfolgt, das Verfahren kam allerdings nur mit technischen Schwierigkeiten in Gang. Fraglich ist bis heute, ob die Ergebnisse den immensen Aufwand, der mit diesen Verfahren verbunden ist, tatsächlich rechtfertigen. Die Senatsverwaltung für Gesundheit und Soziales hat zugesagt, in der ersten Hälfte des Jahres 1999 einen Bericht zu fertigen.

Die Neufassung des *Asylbewerberleistungsgesetzes* vom 5. August 1997[142] hatte auch diesen Personenkreis in die bundesweite Rasterung mit einbezogen. Gleichzeitig mit der Neufassung des AGBSHG wurde auch hier eine landesrechtliche Rechtsgrundlage geschaffen[143]. Auch hier kann man auf die Erfolge der Rasterung gespannt sein.

Konkret umgesetzt werden sollen in Berlin aufgrund von § 117 Abs. 3 BSHG Datenabgleichsverfahren mit dem Landeseinwohneramt, dem Kraftverkehrsamt, den Wohnungsämtern und der Unterhaltsvorschusskasse.

Mit den Vorgaben des § 117 BSHG ist der Rasterhunger allerdings noch nicht gestillt. Immer mehr Ideen kommen auf, wie man auf elektronische Weise der angeblichen Vielzahl von Betrügern auf die Spur kommen könnte. Dabei scheut man auch nicht vor dem Steuergeheimnis zurück: Ein Abgleich der Sozialdaten mit den Berliner Finanzämtern soll zur Rückmeldung der Steuernummern führen; hieraus kann entnommen werden, welche Arten von Steuern vom Sozialhilfeempfänger gezahlt werden und welches Finanzamt zuständig ist (auf die Kfz-Steuer – hier bedient man sich schon des Kraftverkehrsamtes –, die Körperschaftssteuer – so dreist, ein körperschaftssteuerpflichtiges Unternehmen zu führen, wird wohl kein Sozialhilfeempfänger sein – und die Hundesteuer will man großzügig verzichten). Dass die Finanzbehörden Daten an Sozialbehörden nur dann herausgeben dürfen, wenn Tatsachen vorliegen, die zur Aufhebung des Sozialleistungsbescheids führen können (§ 30 a Abs. 3 Abgabenordnung), stört offensichtlich niemanden – im Übrigen auch nicht die Senatsverwaltung für Finanzen als Hüterin des Steuergeheimnisses – die nach wie vor die Geltung des Datenschutzgesetzes für die Steuerverwaltung unter Hinweis auf eben dieses Steuergeheimnis ablehnt[144].

Geldkarte für Asylbewerber und Bürgerkriegsflüchtlinge

Öffentliches Aufsehen hat das Projekt des Landesamtes für Gesundheit und Soziales erlangt, die in Berlin lebenden Asylbewerber mit Chipkarten auszustatten, die eine elektronische Geldbörse enthalten und mit denen die Asylbewerber in bestimmten Geschäften ihren täglichen Bedarf an Lebensmitteln, Hygieneartikeln, Gebrauchs- und Verbrauchsgütern bargeldlos bezahlen können. Bis zur Einführung dieser Karten wurden den Asylbewerbern Sachleistungen gewährt, die gegen die Abgabe von Wertgutscheinen in zwei dafür speziell eingerichteten und bestimmten Läden in Reinickendorf und Kreuzberg empfangen werden konnten. Mit der Chipkarte sollte zu Projektbeginn in mindestens zwei Läden pro Bezirk eingekauft werden können.

Den rechtlichen Hintergrund des Projektes bildet § 3 Asylbewerberleistungsgesetz, wonach *Asylbewerber* nur einen Anspruch auf Sachleistungen oder bargeldlose Leistungen haben. Es wurde daher ein Anbieter gesucht, der das *Chipkartenprojekt* konzipiert, die damit verbundene Datenverarbeitung im Auftrag des Landesamtes für Gesundheit und Soziales durchführt, die Akzeptanzstellen akquiriert, die Händlerterminals installiert sowie die Chipkartenladeeinrichtung im Landesamt betreibt und installiert. Ferner sollte er die Verrechnungen mit den Händlern vornehmen (Clearing) und die regelmäßige Schlussabrechnung mit dem Landesamt durchführen. Da die Entscheidung über die Höhe der gewährten Hilfen weiter dem Landesamt oblag und die Ladebeträge auf den Chipkarten von dem behördlichen Bescheid bestimmt waren, wurden keine hoheitlichen Aufgaben nach außen vergeben, so dass die externe Vergabe nicht gegen datenschutzrechtliche Bestimmungen verstieß.

Die Versorgung der Asylbewerber birgt vielfältige Missbrauchsgefahren, denn es ist ihnen nicht erlaubt, Alkohol oder andere Genussmittel davon zu kaufen oder Waren in Mengen zu kaufen, die den Eigenbedarf überschreiten. Ferner ist in Betracht zu ziehen, dass zum Beispiel noch „offene Rechnungen“ bei Schleppern zu bezahlen sind. Zur *Missbrauchskontrolle* ist der Verwaltungsbehörde durchaus erlaubt, sich ein Bild über das individuelle Kaufverhalten zu machen. Es war aus datenschutzrechtlicher Sicht also darauf zu achten, dass dieser schwer wiegende Eingriff in die informationelle Selbstbestimmung der Asylbewerber durch die Einführung des technischen Systems nicht unverhältnismäßig vereinfacht und ausgedehnt werden kann. Das letztlich eingeführte Verfahren ermöglicht es dem Landesamt für Gesundheit und Soziales nicht, festzustellen, was ein Asylbewerber für den eingespeicherten Geldbetrag gekauft hat. Es können nur die Summenbeträge pro Einkauf und die verbleibenden Ladebeträge über die Zahlungsbelege für die Chipkartenzahlung nachvollzogen werden, Informationen also, die angesichts der Rechtslage datenschutzrechtlich akzeptiert werden können.

Ein wichtiger Aspekt der datenschutzrechtlichen Begleitung des Projekts waren die *sicherheitstechnischen Einrichtungen* des Verfahrens, insbesondere die der Chipkarte zur Verhinderung unrechtmäßiger Nutzung und von Manipulationen. Entsprechend unseren Empfehlungen

142 BGBl. I, 2022
143 a.a.O. Art I: Gesetz zur Ausführung des Asylbewerberleistungsgesetzes
144 vgl. 4.3.2

werden Chipkarten eingesetzt, die den „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entsprechen[145]. Die Bezahlung am Händlerterminal erfolgt mit einer persönlichen Identifikationsnummer.

Gegen diese Konzeption des Einsatzes einer Chipkarte als elektronische Geldbörse für Asylbewerber, bei der alle von uns abgegebenen Empfehlungen umgesetzt wurden, gab es keine datenschutzrechtlichen Einwände mehr. Mit der Einführung des gleichen Zahlungsverfahrens für die von den bezirklichen Sozialämtern betreuten Bürgerkriegsflüchtlinge wurde jedoch erneut ein öffentliche Debatte über das Chipkartenprojekt entfacht, in der deutlich wurde, dass das Verfahren politisch ausgesprochen umstritten ist. Manche Bezirksstadträte verwarfen aus politischen und humanitären Gründen den Einsatz der Chipkarte und machten von der gesetzlichen Option zur bargeldlosen Versorgung keinen Gebrauch, sondern blieben bei der Gewährung des anonym und flexibler handhabbaren Bargelds. Gegen eine solche Entscheidung ist datenschutzrechtlich, natürlich auch ohne nähere Prüfung, nichts einzuwenden.

Ausländerbefragung

Ein weiteres Mal ging es wie schon öfter in der Vergangenheit um die Ausforschung von Kriegsflüchtlingen aus Jugoslawien. Es wurden von einem Berliner Bezirksamt 15 Fragen gestellt, die überwiegend keinen Zusammenhang zur Leistungsberechtigung nach dem Sozialgesetzbuch bzw. nach dem Bundessozialhilfegesetz oder Asylbewerberleistungsgesetz aufwiesen. Vielmehr zielten sie auf Aufgaben der Ausländerbehörde ab.

Dazu gehörten Fragen folgenden Inhalts:

- Wann haben Sie Jugoslawien, Kroatien, Serbien, Bosnien verlassen?
- Wann sind Sie in die Bundesrepublik Deutschland eingereist und über welche Länder?
- Letzter gewöhnlicher Aufenthalt im Ausland (Ort, Land)?
- Warum sind Sie nach Deutschland gekommen?
- Mussten Sie jemanden für die Reise bezahlen? Wenn ja, wen und wie viel?
- Wie lange beabsichtigen Sie in Deutschland zu bleiben?

[145] Das Papier ist beim Berliner Datenschutzbeauftragten erhältlich, Veröffentlichung in der Broschüre „Technik und Datenschutz“ des Landesbeauftragten für den Datenschutz von Mecklenburg-Vorpommern, S. 22–42 und im Internet unter http://www.datenschutz-berlin.de/to/chipkart.htm

- Haben Sie sich seit Bürgerkriegsbeginn in anderen Ländern ausser Deutschland oder dem ehemaligen Jugoslawien aufgehalten? (Wenn ja, wo – Ort, Land)

Ein Sozialamt hat keine Befugnis, derartige Fragen zu stellen. Der *Fragebogen* wurde geändert und auf Fragen beschränkt, die in unmittelbarem Zusammenhang mit der Leistungsgewährung und mit der Prüfung der Bedürftigkeit stehen.

Die verlorene Akte

Ein Petent hatte Dienstaufsichtsbeschwerde wegen der erheblich verzögerten Bearbeitung seines Widerspruchs in einem Pflegegeldvorgang eingelegt. Nach Feststellungen der betroffenen Stelle wurde sein Widerspruch mit dem Pflegegeldvorgang, der den gesamten Schriftwechsel einschließlich ärztlicher Gutachten enthielt, zur Begutachtung und Überprüfung an den Ärztlichen Dienst des Landesamtes für Zentrale Soziale Aufgaben weitergeleitet, war aber dort nicht auffindbar. Ein Verschulden der Mitarbeiterinnen und Mitarbeiter der absendenden Stelle wurde nicht festgestellt und die Dienstaufsichtsbeschwerde als unbegründet zurückgewiesen.

Nach dieser Stellungnahme bleibt beim Bürger mit Recht ein bitterer Nachgeschmack von Enttäuschung und Hilflosigkeit zurück, weil die Stellungnahme nichts erklärt und die Unterlagen des Pflegegeldvorgangs nach wie vor verschwunden bleiben. Auch wir konnten natürlich nicht die beteiligten Verwaltungen des Landes und den Fachpostverkehr durchkämmen, um dem mit Recht erzürnten Petenten die Akte wieder zu verschaffen. Auch der formale Gesichtspunkt, dass die absendende Stelle grundsätzlich die Gefahr der Datenübermittlung trägt, hilft nicht weiter, weil bei *verlorenen Unterlagen* die Gefahr eines unersetzlichen Verlustes besonders schwer wiegend ist und Beweismaterialien des Bürgers unwiderruflich verloren gehen können. Zudem besteht die Gefahr, dass die sensiblen Unterlagen in unbefugte Hände geraten können. Auch können sich erhebliche Haftungsrisiken für die Verwaltung ergeben, so dass es dringend angezeigt scheint, *Transportkontrollen* bzw. Kontrollmöglichkeiten zu entwickeln, um den Verbleib von Unterlagen so weit wie möglich nachprüfen zu können. Der Verlust der Akte darf keinesfalls dazu führen, dass dem Bürger berechtigte Ansprüche verloren gehen.

Unterhalt für die Schwiegermutter

Großes Erstaunen zeigte die Ehefrau eines für seine Mutter unterhaltspflichtigen Ehemannes, als sie von ihrem Arbeitgeber die Nachricht erhielt, dass das Sozialamt sich nach ihrer Einkommenshöhe erkundigt hatte. Da die Ehefrau im Gegensatz zu ihrem Mann nicht unterhaltspflichtig ist, hatten sich beide entschlossen, nur die Einkommensver-

hältnisse des Mannes dem Sozialamt anzugeben. Trotzdem wurden sie aufgefordert, ihre gesamten Einkommensverhältnisse aufzudecken, also auch diejenigen der Frau. Diese wollte wissen, woher das Sozialamt die Informationen über sie bekommen hatte, um ihren Arbeitgeber anzuschreiben.

Das Bezirksamt hat beim Einwohnermeldeamt den Familienstatus des unterhaltspflichtigen Mannes abgeklärt. Daraufhin wurde bei der Bundesversicherungsanstalt für Angestellte in Erfahrung gebracht, wer der Arbeitgeber der Ehefrau war. An diesen Arbeitgeber wurde daraufhin das Auskunftsersuchen gerichtet. Zuvor war der Ehemann durch Mahnung und Fristsetzung aufgefordert worden, die Angaben über die Einkommensverhältnisse seiner Frau nachzuliefern. Die Eheleute hatten nicht reagiert. Somit waren die Voraussetzungen sowohl des § 74 SGB X wie auch des § 116 Abs. 2 BSHG gegeben. Danach muss die nichtunterhaltspflichtige Frau ihre Einkommensverhältnisse angeben. Sie ist zwar nicht unterhaltspflichtig, jedoch unterliegen aufgrund ihrer eigenen Einkommensverhältnisse diejenigen des unterhaltspflichtigen Mannes einer besonderen Bewertung.

Datenschutz und Befangenheit

Eine Petentin hatte Wohngeld beantragt. Sie wurde wenig später vom Wohngeldamt aufgefordert, ihren letzten Kontoauszug mit einem bestimmten Überweisungsbeleg einzureichen. Unterzeichnet war das Schreiben des Wohngeldamtes von einer Person, die ebenfalls Bewohnerin des Hauses war, in dem die Petentin wohnte. Auf diese Tatsache hingewiesen, zeigte der Leiter des Wohngeldamtes kein Verständnis für den Einwand und beließ die Bearbeitung bei der Nachbarin.

Dieser Fall wirft die Frage auf, in welchem Verhältnis der Datenschutz zu den verfahrensrechtlichen Vorschriften zur *Befangenheit* steht (§ 21 Verwaltungsverfahrensgesetz). Liegt ein Grund vor, der geeignet ist, Misstrauen gegen eine unparteiische Amtsausübung durch eine Dienstkraft zu rechtfertigen, so hat diese sich „der Mitwirkung zu enthalten“, d. h. sie ist auch von der Kenntnis entsprechender Vorgänge auszuschließen. Ob das bloße Mitbewohnen des gleichen Hauses schon genug Grund abgibt, von der Befangenheit eines Mitarbeiters auszugehen, ist allerdings fraglich. Er könnte beispielsweise zu bejahen sein, wenn persönliche Verflechtungen in dem Haus gegeben sind. Handelt es sich jedoch um große Wohneinheiten, wo so viele Menschen wohnen, dass sie einander kaum kennen, so kann das bloße Mitbewohnen kaum als Befangenheitsgrund angesehen werden.

Wenn es die Verhältnisse zulassen, sollte allerdings in derartigen Fällen gleichwohl nach einer Lösung gesucht werden, die eine Einsichtnahme in die Unterlagen der Nachbarin vermeidet. Zumindest sind nach § 78 a SGB X die Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Sozialgesetzbuchs zu gewährleisten. Zu derartigen Maßnahmen würde in dem hier geschilderten Fall gehören, dass die betreffende Mitarbeiterin besonders auf die Einhaltung der datenschutzrechtlichen Verpflichtungen hingewiesen und belehrt wird.

Ähnlich lag der Fall bei einer Mitarbeiterin der Senatsverwaltung für Wirtschaft und Betriebe, die einen Feststellungsantrag zur Schwerbehinderung beim Landesamt für Gesundheit und Soziales gestellt hatte und plötzlich davon unterrichtet wurde, dass Bewilligungsbescheide und sonstiger Schriftverkehr des Landesamtes für Gesundheit und Soziales von Mitarbeiterinnen der Senatsverwaltung für Wirtschaft und Betriebe geschrieben werden sollten, um Spitzenlasten beim Landesamt abzubauen.

In diesem Fall verbietet das Sozialgeheimniss unabhängig von dem Zufall, dass die Antragstellerin just in der Dienststelle beschäftigt war, die die Aufgaben übernahm, so vorzugehen. Die Praxis wurde geändert.

Schwarzarbeit und ihre Datenspuren

Bekanntlich schafft die kaum überschaubare Dimension der *Schwarzarbeit* erhebliche Probleme. Die zunehmende Verschärfung der Kontrollen hinterlässt auch Datenspuren im Berliner Verwaltungsgetriebe. Im Interesse einer effizienten Nachprüfung melden die Polizeibehörden, die bei ihren Kontrollen auf Baustellen Schwarzarbeiter vorgefunden haben, deren Namen an eine „Verbindungsstelle“, damit von dort aus die zuständige bezirkliche Sozialverwaltung ermittelt werden kann. Diese Amtshilfe ist datenschutzrechtlich unbedenklich, da sie zu einer höheren Effizienz und Genauigkeit bei der Weiterleitung der personenbezogenen Datensätze führt. Die zuständigen Leistungsträger können dann die erforderlichen weiteren Maßnahmen, wie z. B. Regressansprüche, Leistungsstopp, Strafanzeige, prüfen und nach eigenem rechtlichem Ermessen durchsetzen.

Die zuständige Senatsverwaltung benötigt jedoch *Rückmeldungen* über die Effizienz der ergriffenen Maßnahmen, um die Kontrollarbeit richtig bewerten zu können. Es liegt auch im datenschutzrechtlichen Interesse, dass die weit reichenden Kontrollbefugnisse, die ja mit erheblichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung verbunden sind, einer ständigen Erfolgskontrolle unterzogen werden, um die Fortdauer der Zulässigkeit und Effizienz dieser Maßnahmen belegen zu können. Die Verbindungsstelle hatte hierzu Formulare entwickelt, mit denen unter Angabe des Namens des Verdächtigten die Verbindungsstelle informiert werden sollte, welche Maßnahmen mit welcher Erfolgsaussicht ergriffen wurden.

Da die Verbindungsstelle ihrerseits jedoch solche Maßnahmen weder bewerten noch beeinflussen sollte, war die Übermittlung der Namen von Betroffenen auf dem Melderückweg von den Sozialämtern an die

Verbindungsstelle nicht erforderlich und daher unzulässig. Es ist kurzfristig mit der Verbindungsstelle und der beteiligten Senatsverwaltung für Soziales ein Verfahren unter unserer Mitwirkung entwickelt worden, bei dem die *Anonymität der betroffenen Personen* bei dem Melderückweg gewährleistet wurde und gleichzeitig eine Effizienzkontrolle durch die Verbindungsstelle durchgeführt werden kann.

Eine Geschichte, die das Leben schrieb

Eine große Liebe auf der Flucht im Januar 1945 über die Ostsee zwischen einer jungen Frau und einem Soldaten. Das Leben erzwingt die Trennung. Die junge Frau heiratet einen anderen Mann. Sehr bald bekommt sie einen Sohn. Diesem berichtet sie auf dem Sterbebett im Jahre 1998 von ihrer Liebe und gesteht dem Sohn zum ersten Mal, dass nicht der geheiratete Mann sein Vater ist, sondern jener, den sie auf der Flucht kennen gelernt hatte. Sie hinterlässt dessen Foto mit einer handschriftlichen Signierung und dessen Namen sowie Anhaltspunkten über den zuständigen Truppenteil, dem er als Soldat angehörte.

Über die *Deutsche Dienststelle* (WASt) für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Deutschen Wehrmacht versuchte der Sohn die Anschrift und Identität des vermuteten Vaters zu klären. Die WASt ermittelt tatsächlich einen noch lebenden Mann, auf den diese Angaben passen und fragt bei ihm an, ob er einverstanden sei, dass seine Anschrift herausgegeben werde. Dieser lehnt ab.

Die WASt ist berechtigt, personenbezogene Daten an Privatpersonen auch ohne Einwilligung herauszugeben, wenn „das Interesse an der Aufklärung des Einzelschicksals die schutzwürdigen Belange des Betroffenen erheblich übersteigt“ (§ 6 WASt-Verordnung)[146]. Entgegen ihrer Bezeichnung hat die WASt auch Aufgaben hinsichtlich lebender Personen zu erfüllen, so z. B. für Dienstzeitennachweise, Erbrechtsangelegenheiten oder, wie hier, *Vaterschaftsfeststellungsverfahren* (§ 2 Ziff. 12 WAStG).

Es ist anerkannt, dass das Recht des Menschen, seine Abstammung zu erfahren, ein Grundrecht ist[147]. Dem Interesse des Sohnes, seinen Vater ausfindig zu machen, ist daher hohe Bedeutung beizumessen. Wir haben der Deutschen Dienststelle empfohlen, den vermeintlichen Vater über die Rechtslage in Kenntnis zu setzen, um ihn über etwaige weitere Schritte der WASt vorab zu informieren. Insbesondere empfahlen wir darauf hinzuweisen, dass die Deutsche Dienststelle befugt ist, die

146 Die Verordnung über die Verarbeitung personenbezogener Daten bei der Deutschen Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen Deutschen Wehrmacht vom 29. März 1994, GVBl. S. 107, ist erlassen aufgrund des Gesetzes über die Verarbeitung von personenbezogenen Daten bei der WASt v. 26. Januar 1993, GVBl. S. 40, 49

147 Beschluss v. 6. 5. 1997, – BvR 409/90, BVerfGE 79, 256 (269)

Adresse an den vermeintlichen Sohn zu offenbaren, wenn nicht überwiegende schutzwürdige Belange von ihm als vermeintlichem Vater geltend gemacht werden. Wir meinen, dass eine solche Interessenlage einer genauen Prüfung bedarf, dass aber letztlich das überwiegende Interesse des Sohnes nach Kenntnis seiner wahren Abstammung nur schwer durch höherrangige schutzwürdige Belange des Vaters übertroffen werden kann. Auf diese Weise ist es dann gelungen, dass Vater und Sohn sich begegnen konnten.

4.4.4 Bauen, Wohnen und Umwelt

Neue Verordnung zur Durchführung des Baugesetzbuches (DVO-BauGB)

Die neue DVO-BauGB[148] enthält Regelungen zur Bodenordnung (Umlegung), Wertermittlung (Gutachterausschuss für Grundstückswerte in Berlin) und Enteignung (Enteignungsbehörde). Die Neufassung war dringend erforderlich, um die Bestimmungen der aktuellen Entwicklung – insbesondere im Abschnitt Wertermittlung – anzugleichen. Grundlage für die Tätigkeit des *Gutachterausschusses für Grundstückswerte* in Berlin und seiner bei der Senatsverwaltung für Bauen, Wohnen und Verkehr eingerichteten Geschäftsstelle ist die Kaufpreissammlung. Diese enthält die wesentlichen Daten aus den übersandten Grundstückskaufverträgen (vgl. § 195 Baugesetzbuch [BauGB]). Die Einführung eines neuartigen DV-Systems zur Führung einer *automatisierten Kaufpreissammlung* (AKS) war der Anlass, die Regelungen zur Kaufpreissammlung in der DVO-BauGB den datenschutzrechtlichen Erfordernissen anzupassen. Dies erfolgte in Abstimmung zwischen der Senatsverwaltung für Bauen, Wohnen und Verkehr und uns. Wir konnten bereits in einem frühen Entwurfsstadium der Verordnung unsere Empfehlungen einbringen, die auch im Wesentlichen berücksichtigt wurden.

Nach der neuen Fassung werden *Auskünfte aus der Kaufpreissammlung* (§ 18 DVO-BauGB) nur noch in Form anonymisierter Daten erteilt, wenn ein berechtigtes Interesse vorliegt. Darüber hinaus können bestimmte Berufsgruppen (z. B. öffentlich bestellte Vermessungsingenieure) auf anonymisierte Daten der Kaufpreissammlung zugreifen. Die Daten sind anonymisiert, wenn sie nicht auf bestimmbare Personen und Grundstücke bezogen werden können. Die Anonymität der Daten ist programmtechnisch und organisatorisch zu gewährleisten. Die auf bestimmbare Personen und Grundstücke beziehbaren Daten in der Kaufpreissammlung sind gesperrt. Zugriffe auf die Kaufpreissammlung sind zur Datenschutzkontrolle automatisiert zu protokollieren (§ 17 Abs. 5 DVO-BauGB). Die protokollierten Daten dürfen nur zu diesem Zweck genutzt werden und sind nach zwei Jahren zu vernichten.

148 vom 5. November 1998 (GVBl S. 331)

Damit wurde den Bedürfnissen nach mehr Transparenz am Grundstücksmarkt und einem kundenorientierten Informationsangebot des Gutachterausschusses – unter Beachtung der datenschutzrechtlichen Belange – Rechnung getragen. Inwieweit dieser Interessenausgleich auch bei dem geplanten, weiterführenden Projekt, Daten des Gutachterausschusses im Internet zu veröffentlichen *(GAA-Online),* möglich ist, bleibt abzuwarten.

Veröffentlichung von Mitgliederdaten im Handbuch der Architektenkammer Berlin

Die Architektenkammer gibt im Abstand von ein bis zwei Jahren ein „Handbuch Architektenkammer Berlin" heraus. Darin werden diejenigen Mitglieder der Architektenkammer getrennt nach Fachbereich und Tätigkeitsart verzeichnet, die zuvor auf einem Erhebungsbogen die Erlaubnis zur Veröffentlichung erteilt haben. Von einem Architekten-Verband wurde der Vorstand aufgefordert, zukünftig alle Mitglieder im Handbuch zu verzeichnen – unabhängig davon, ob die Betroffenen einer Veröffentlichung widersprochen haben oder nicht.

Die Veröffentlichung der *Mitgliederdaten im Handbuch* ist eine Übermittlung an eine unüberschaubare Anzahl von Dritten. Nach § 13 BlnDSG ist das nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat. Nach § 18 Abs. 2 Satz 2 Berliner Architekten- und Baukammergesetz darf die Architektenkammer Daten nur insoweit veröffentlichen, als diese Daten auch aus anderen Quellen allgemein zugänglich sind. Dies trifft unter Umständen auf Angaben zum Namen, zur Anschrift und zu Telefon- bzw. Telefaxnummern zu, die u. a. aus den Telefonverzeichnissen der Telekom zu entnehmen sind. Darüber hinaus werden im „Handbuch Architektenkammer Berlin" jedoch auch Angaben zum Fachbereich und zur Tätigkeitsart der betroffenen Mitglieder veröffentlicht. Diese Angaben sind nicht aus anderen allgemein zugänglichen Quellen zu entnehmen.

Die Veröffentlichung der Daten und Angaben zur Person der Kammermitglieder, die allgemein zugänglich sind, ist jedoch nur zulässig, sofern der Betroffene der Veröffentlichung nicht widersprochen hat (§ 18 Abs. 2 Satz 3 Berliner Architekten- und Baukammergesetz) und hinsichtlich des vollen Datenumfangs kann das Verfahren nur beibehalten bleiben, wenn die Mitglieder zuvor ihre Erlaubnis dazu erteilt haben.

Säumige Mieter werden an den Pranger gestellt

In einem regelmäßig erscheinenden Informationsblatt, das an alle Mitglieder übersandt wird, hat eine Wohnungsbaugenossenschaft die Namen und Anschriften von Mitgliedern veröffentlicht, deren Wohnungen wegen Mietrückständen geräumt bzw. die aus der Genossenschaft ausgeschlossen werden sollen.

Diese Veröffentlichung stellt eine Übermittlung personenbezogener Daten der Betroffenen an Dritte – hier: Die Leser des Informationsblattes – dar und ist nach § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) nur zulässig, wenn das BDSG selbst oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene darin eingewilligt hat.

Die Übermittlung von Angaben über den aktuellen Mitgliederstand in der *Genossenschaft* ist abschließend in § 31 Abs. 1 Genossenschaftsgesetz (GenG) geregelt. Danach kann die *Mitgliederliste* von jedem Genossen sowie von einem Dritten, der ein berechtigtes Interesse darlegt, bei der Genossenschaft eingesehen werden. Abschriften aus der Mitgliederliste kann der Genosse nur hinsichtlich der ihn betreffenden Eintragungen verlangen. Damit hat der Gesetzgeber mit gutem Grund – zum Schutz der Betroffenen – abschließend die Übermittlung der Daten aus der Mitgliederliste durch Einsichtnahme und Fertigung von Abschriften in bestimmten Ausnahmefällen vorgesehen. Für eine Veröffentlichung der Daten in einem Informationsblatt bleibt kein Raum; sie ist unzulässig.

Die Veröffentlichung von Mieternamen und Anschriften im Zusammenhang mit Zwangsräumungen ist ebenfalls unzulässig. Weder das Genossenschaftsgesetz noch das BDSG enthält eine Rechtsgrundlage, auf die diese Übermittlung von personenbezogenen Daten gestützt werden könnte. Andere Rechtsvorschriften, die die Übermittlung erlauben oder anordnen, sind ebenfalls nicht ersichtlich. Wir haben die Wohnungsbaugenossenschaft aufgefordert, zukünftig keine derartigen Angaben in Informationsblättern zu veröffentlichen.

Auskunft aus dem Liegenschaftskataster

Aufgrund mehrerer Eingaben haben wir uns mit der besonderen Rechtslage in Berlin befasst, die dazu geführt hat, dass die Auskunft aus dem bzw. die Einsicht in das Grundbuch und das Liegenschaftskataster unterschiedlichen Voraussetzungen unterliegen.

Das Grundbuch hält die rechtliche Lage eines Grundstückes für die Öffentlichkeit fest. Wegen des daraus folgenden Publizitätsgrundsatzes knüpft das Sachenrecht an eine Eintragung im Grundbuch Vermutungs- und Gutglaubensschutzwirkungen. Eine Einsicht in das *Grundbuch* wird vom Grundbuchamt bei Geltendmachung eines berechtigten Interesses (§ 12 Grundbuchordnung [GBO]) gewährt.

Dagegen sind im *Liegenschaftskataster* die vermessenen Grundstücke, die örtliche Lage und die Zuordnung der einzelnen Grundstücke zueinander aufgeführt. Es dient in erster Linie raumplanerischen und städtebaulichen Zwecken. Um diese Zwecke erfüllen zu können, muss das Liegenschaftskataster auch die rechtliche Lage – also Eigentümer, grundstücksgleiche Rechte und Gebäude – darstellen. Im Liegenschaftskataster ist somit nicht nur die tatsächliche, sondern auch die

rechtliche Lage des Grundstückes entsprechend den Eintragungen im Grundbuch abgebildet. Nach § 17 Abs. 1 Vermessungsgesetz Berlin (VermGBln) ist jeder berechtigt, aus dem Liegenschaftskataster schriftliche Auskünfte über einzeln bestimmte Liegenschaften zu erhalten. Die Glaubhaftmachung eines berechtigten Interesses ist – im Gegensatz zur Einsicht in das Grundbuch – nicht erforderlich.

Die unterschiedlichen Voraussetzungen zur Auskunftserteilung sind anzugleichen. Anderenfalls besteht die Möglichkeit, die von § 12 GBO geforderte Glaubhaftmachung eines berechtigten Interesses an den Grundbuchdaten über einen Antrag auf Auskunft aus dem Liegenschaftskataster zu umgehen. Ein Vergleich der rechtlichen Bestimmungen in den anderen Bundesländern hat ergeben, dass nur in Berlin keine einschränkenden rechtlichen Voraussetzungen für die Auskunft aus dem Liegenschaftskataster bestehen. In allen anderen Bundesländern besteht für Dritte die Verpflichtung, ein berechtigtes Interesse an der Auskunft aus dem Liegenschaftskataster glaubhaft darzulegen.

Wir haben der Senatsverwaltung für Bauen, Wohnen und Verkehr empfohlen, eine Initiative zu ergreifen, damit die Bestimmung des § 17 Abs. 1 VermGBln der Rechtslage in den anderen Bundesländern angepasst wird. Dies wurde abgelehnt.

Auslegung von Grundstücksverzeichnissen im Planfeststellungsverfahren

Im „Länderfachausschuss Straßenbaurecht“ wurde eine bundeseinheitliche Regelung der datenschutzrechtlichen Anforderungen im Planfeststellungsverfahren angestrebt. Unter anderem wurde diskutiert, ob anlässlich der *öffentlichen Planauslegung* (§ 73 VwVfG) die Vorlage eines *Verzeichnisses* mit Name, Vorname und Anschrift *der betroffenen Grundstückseigentümer* erforderlich und zulässig ist. Unsere Kritik, dass diese Vorgehensweise weder auf die Einwilligung der Betroffenen noch auf eine Rechtsgrundlage (vgl. § 13 BlnDSG) gestützt werden kann, wurde von der Senatsverwaltung für Bauen, Wohnen und Verkehr aufgegriffen. Danach werden in Berlin in den anstehenden Planfeststellungsverfahren bei der öffentlichen Auslegung in den datenschutzrechtlich relevanten Unterlagen, insbesondere dem Grunderwerbsverzeichnis, Name, Vorname und Anschrift der Grundstückseigentümer mit Nummern verschlüsselt. Den Grundstückseigentümern wird die ihr Grundstück betreffende Verschlüsselungsnummer mitgeteilt.

Einkommensabhängige Wohnungsbauförderung

Anlässlich der Neufassung der Förderrichtlinien zur einkommensorientierten Wohnungsbauförderung haben wir uns mit der Verarbeitung von Mieterdaten befasst. Nach § 88 e Abs. 3 Satz 3 Zweites Wohnungsbaugesetz (II. WoBauG) ist der antragstellende Vermieter Empfänger der Zusatzförderung. Diese wird dem Vermieter ausschließlich zur Verringerung des von den bezugsberechtigten Mietern zu zahlenden Mietzinses überwiesen.

Im Vordergrund der datenschutzrechtlichen Bewertung steht der Umstand, dass der Mieter nach § 88 e Abs. 3 Satz 2 II. WoBauG die *für die Berechnung der Förderung erforderlichen Nachweise* (zur Berechnung der Einkommensgrenze nach § 25 II. WoBauG) zu erbringen hat. Fraglich ist, ob der Mieter diese Nachweise – die zum Teil personenbezogene Daten, z. B. zum Einkommen, enthalten – über den Vermieter oder direkt an die Bewilligungsstelle einzureichen hat.

Nach § 10 Abs. 1 BlnDSG hat die Erhebung von personenbezogenen Daten grundsätzlich bei dem Mieter mit seiner Kenntnis zu erfolgen. Danach ist dem Mieter von der Bewilligungsstelle die Möglichkeit einzuräumen, die Nachweise im Rahmen von § 25 II. WoBauG direkt – ohne Umweg über den Vermieter – einzureichen. Nur dadurch kann eine Kenntnisnahme durch den Vermieter ausgeschlossen werden. Sowohl Vermieter als auch Mieter sind über diese Möglichkeit der Datenübermittlung im Antragsverfahren ausreichend zu informieren. Nachdem ein entsprechendes Verfahren bereits bei der Datenerhebung zur Freistellung bzw. Ausgleichszahlung nach § 7 Wohnungsbindungsgesetz (WoBindG) und der Gewährleistung von Aufwendungszuschüssen für familiengerechte Miet- und Genossenschaftswohnungen erfolgreich und problemlos praktiziert wird, hat die Senatsverwaltung für Bauen, Wohnen und Verkehr angekündigt, dass die Mieter ihre Nachweise zur einkommensorientierten *Wohnungsförderung* zukünftig auch direkt bei der *Investitionsbank Berlin (IBB)* – ohne Umweg über den Vermieter – einreichen können. Mieter und Vermieter werden durch einen Textzusatz im Vordruck „Anlage zum Mietvertrag“ ausreichend über die Möglichkeit informiert.

Datenerhebungen für kommunales Vorkaufsrecht

Unter bestimmten Voraussetzungen stehen dem Land Berlin kommunale Vorkaufsrechte bei Grundstücksverkäufen zu. Nimmt das Land diese Rechte nicht wahr, erteilt es so genannte Negativzeugnisse. Zur Durchführung des Verfahrens wurde – ohne Ausnahme – die Vorlage der vollständigen Urkundsabschriften der Kaufverträge verlangt, ohne zuvor geprüft und festgestellt zu haben, ob überhaupt ein kommunales Vorkaufsrecht in Betracht kommt.

Diese Verfahrensweise ist weder erforderlich noch verhältnismäßig[149]. Die Senatsverwaltung für Bauen, Wohnen und Verkehr hat die Problematik im Rundschreiben II Nr. 1/1998 an alle Bezirksämter des Landes Berlin aufgegriffen und diese gebeten, das von uns empfohlene zweistufige Verfahren umzusetzen.

149 JB 1995, 5.2

Danach genügt es für die *Erteilung des Negativzeugnisses,* wenn aus dem Inhalt des Kaufvertrages die Daten über den Kauf, die Kaufvertragsparteien und die genaue Bezeichnung des Grundstücks vorliegen. Wird nach Prüfung festgestellt, dass kein Vorkaufsrecht besteht, wird innerhalb der Zweimonatsfrist nach § 28 Abs. 2 BauGB ein Negativzeugnis erteilt. Erst wenn aufgrund der Informationen festgestellt wird, dass ein gesetzliches Vorkaufsrecht des Landes Berlin besteht und seine Ausübung in Betracht kommt, kann die Übermittlung des vollständigen Kaufvertrages gefordert werden.

Datenverarbeitung bei Bewerbungen um Mietwohnungen

Im Jahresbericht 1996[150] haben wir über die Datenverarbeitungspraxis der Vermieter bei *Wohnungsbewerbungen* berichtet. Die Auswertung zahlreicher *Fragebögen,* die von Berliner Vermietern zu diesem Zweck genutzt werden, ergab, dass nur wenige den gesetzlichen Vorgaben zur Verarbeitung von personenbezogenen Daten der Bewerber entsprachen. Nachdem zunächst der Verband Berlin-Brandenburgischer Wohnungsunternehmen unserer rechtlichen Bewertung im wesentlichen zugestimmt hatte, hat sich nunmehr auch die Senatsverwaltung für Bauen, Wohnen und Verkehr dieser Auffassung angeschlossen.

In einem Rundschreiben an alle Wohnungsbaugesellschaften des Landes Berlin wurden diese aufgefordert, ihre Fragebögen für Mietwohnungsbewerber entsprechend den datenschutzrechtlichen Vorgaben zu aktualisieren.

Erhebung von Umweltdaten und Nutzung zu fremden Zwecken

Im Auftrag eines Bezirksamtes wurde von einer Privatfirma eine Bestandserfassung ökologischer Daten und deren Aktualisierung im Vergleich mit vorhandenen Daten für öffentliche Grün- und Erholungsanlagen durchgeführt. Dazu wurden in ausgewählten Kleingarten- und Dauerwohnanlagen des Bezirkes Erhebungen durchgeführt mit dem Ziel, Erkenntnisse über die Bodenversiegelung, Vegetation und die gegenwärtige Nutzung der Grundstücke zu gewinnen. In Abstimmung mit den Nutzern der Grundstücke wurden zu diesem Zweck umfangreiche personenbezogene Daten – u. a. Name, Grundstück, Bebauung (z. B. Wohnhaus, Garage oder Carport usw.), vorhandene Medien, Vegetationsbestand – erhoben und verarbeitet. Nach Abschluss des ökologischen Projektes wurden die Daten dem von dem Bezirksamt eingesetzten Verwalter der verpachteten Grundstücke übermittelt, der diese seitdem für Zwecke der Verwaltung (Berechnung von Nutzungsentgelt, Abrissverfügungen für nichtgenehmigte Anlagen usw.) nutzt.

150 JB 1996, 3.3

Eine derartige *zweckfremde Nutzung* der Daten durch das Bezirksamt ist nicht zulässig, da keine Rechtsvorschrift besteht, die dies vorsieht oder zwingend voraussetzt (vgl. § 6 Abs. 2 BlnDSG i.V.m. § 14 Abs. 2 BDSG). Zudem widerspricht die Weitergabe und zweckfremde Nutzung der Daten dem Grundsatz von Treu und Glauben, der bei jeder Erhebung von personenbezogenen Daten zu berücksichtigen ist. Danach ist dem Betroffenen der konkrete Erhebungszweck anzugeben. Die Betroffenen wurden jedoch ausschließlich über eine Nutzung der Daten im Rahmen des *ökologischen Projektes* informiert. Der Umstand, ob das Land Berlin als Eigentümer der Grundstücke grundsätzlich berechtigt ist, Angaben über die Bebauung der Grundstücke zu erheben und diese für Verwaltungszwecke zu nutzen, ist für die datenschutzrechtliche Bewertung nicht erheblich. Entscheidend ist vielmehr, dass die Daten gerade nicht zu diesem Zweck erhoben worden sind.

4.5 Wissen und Bildung

4.5.1 Wissenschaft und Forschung

Hochschulautonomie auch in Datenschutzfragen

Das Berliner Hochschulgesetz ermächtigt die Hochschulen über den Rahmen des Hochschulgesetzes und der Studentendatenverordnung hinaus, sich durch Satzung die Befugnis zu geben, weitere erforderliche personenbezogene Daten für Zwecke der Forschung und Lehre zu verarbeiten. Wir berichteten[151] über eine Satzung der Freien Universität Berlin, die für die Nutzer der Datenverarbeitungsressourcen und der Universitätsbibliothek wesentliche Vereinfachungen bringt. Die Humboldt-Universität zu Berlin erwog nunmehr eine *Dokumentation von Abschlussarbeiten* einer bestimmten Thematik. Derzeit werden diese Arbeiten lediglich bei den Prüfungsämtern für Zwecke der Nachvollziehbarkeit der erbrachten Leistungen gespeichert. Es existiert keine Dokumentation der Verfasser, der Themen und des Inhalts von Diplom- und Magisterarbeiten sowie anderer Abschlussarbeiten. Um diesen bislang brachliegenden Fundus wissenschaftlicher Erkenntnisse öffentlich nutzbar zu machen, kann in einer Satzung geregelt werden, in welchem Umfang, für welche Zwecke insbesondere Übermittlungen, Veröffentlichungen und der Zugriff Interessierter erfolgen dürfen. Wenn von anderen Wissenschaftlern der Wunsch besteht, mit den Autoren in Kontakt zu treten, könnte die Hochschule durch *Adressmittlung*[152] den Kontakt herstellen. Es ist aber auch vorstellbar, dass Studenten Interesse daran haben, dass ihre Abschlussarbeiten ausschließlich zur Dokumentation ihrer Prüfungsleistung genutzt werden. Zur Wahrung dieser Belange ist in die Satzung eine Widerspruchsklausel aufzunehmen.

151 JB 1997, 4.5.1

152 siehe u. a. Materialien zum Datenschutz Heft 18 „Datenschutz in Wissenschaft und Forschung", S. 25

Unser Vorschlag wurde an einigen Berliner Universitäten und Hochschulen aufgegriffen. Die behördlichen Datenschutzbeauftragten dieser Einrichtungen haben Anforderungen an eine *Mustersatzung* erarbeitet. Die spezifischen datenschutzrechtlichen Regelungen der einzelnen Hochschule sollten in möglichst nur einer Satzung zusammengefasst werden. Diese kann dann flexibel den Veränderungen in der Hochschule und ihrer Organisation angepasst, ergänzt oder revidiert werden.

Chipkarten für Berliner Studenten

Die *Chipkarten-Projekte* im Bereich der Berliner Hochschulen, zu denen wir im Vorjahr zum Stichwort „Der ‚gläserne' Student" bereits berichtet hatten[153], sind weiter vorangetrieben worden, ohne dass es bereits zum Einsatz solcher Medien gekommen wäre.

Federführend bei dem Versuch, ein einheitliches Verfahren in den Berliner Hochschulen einzuführen, ist die Technische Fachhochschule Berlin. In Zusammenarbeit mit der Landesbank Berlin und einem Berliner Systemhaus soll ein *Studierenden-Ausweis* auf der Basis einer Chipkarte mit elektronischer Geldbörse entwickelt werden. Neben der federführenden Fachhochschule kooperieren dabei die Freie Universität, die Humboldt-Universität, die Technische Universität, die Hochschule der Künste, die Fachhochschule für Technik und Wirtschaft und die Fachhochschule für Wirtschaft.

Wir haben zu dem Projekt datenschutzrechtliche und IT-sicherheitstechnische Anforderungen formuliert, die notwendig sind, um den „gläsernen Studenten" sowohl in seiner Rolle als Hochschulangehöriger als auch als Konsument zu verhindern:

- Das Datenmodell auf der Chipkarte sieht zwei Dateien „Stammhochschule" und „Hochschulzugehörigkeit" vor, die technisch voneinander abgeschottet sind. Die Datei „Stammhochschule" enthält u. a. die Matrikel-Nummer und ermöglicht die Erschließung weiterer Daten und Anwendungen in Hintergrundsystemen von Hochschulen. Dagegen enthält die Datei „Hochschulzugehörigkeit" die Matrikel-Nummer nicht und kann so außerhalb der Hochschulen für den Nachweis der Hochschulzugehörigkeit genutzt werden.
- Im sichtbaren Bereich enthält die Chipkarte neben den Angaben zum Namen, Vornamen und zur Hochschule ein Lichtbild, einen Barcode zur Benutzung der Bibliotheken sowie einen Thermochronik-Streifen für die Aufnahme änderbarer, lesbarer Angaben zum Gültigkeitszeitraum.
- Da nach § 6 Abs. 7 Berliner Hochschulgesetz die Hochschulen für die Benutzung ihrer Einrichtungen nur Namen, Anschrift und Geburtsdatum verarbeiten dürfen, müssen Hochschulen, die auch die Matrikel-Nummer für diese Zwecke verwenden wollen, dies in einer Satzung zulassen. Eine Nutzung im Personalbereich findet noch nicht statt und bedarf weiterer datenschutzrechtlicher Erörterungen.
- Die Geldkartenfunktion beruht auf der konto-ungebundenen „White-Card"-Funktion, die absolut anonyme Zahlungen ermöglicht.
- Fälschungssicherheit und Kartenauthentität werden nach dem Stand der Technik mit Challenge-Response-Verfahren gewährleistet.

[153] JB 1997, 4.5.1

Zerstreute Dozenten?

Aufgrund einer Eingabe prüften wir den Umgang mit Studentendaten in Fachbereichs- und Institutssekretariaten einer Hochschule. Uns war mitgeteilt worden, dass von den Studenten zum Teil neben der Angabe von Namen, Vornamen und Matrikelnummer auch die Abgabe eines Fotos gefordert wird, um eine Teilnahmebescheinigung zu erhalten. Wir fanden eine bis in die Jahre 1984/85 zurückreichende Kartei, die überwiegend mit Fotos der Studenten versehen war. Anderen Fachbereichen genügte der Eintrag in eine Liste. Der zuständige Dozent benotete nach Abschluss der Prüfungen oder Praktika die Leistungen und bestätigte dies auf der Liste. Durch das Sekretariat wurden dann die Scheine ausgestellt und vom Dozenten den Studenten übergeben. Ein weiterer Fachbereich nutzte ein perforiertes Blatt, das von den Studenten selbst ausgefüllt wurde. Der Dozent bestätigte die Studienleistung, der obere Teil des Blattes verblieb als Nachweis in den Sekretariaten. Die Studenten holten sich ihre Scheine dann unter Vorlage des Studentenausweises im Sekretariat ab.

Die Hochschule reagierte umgehend auf die von uns festgestellten Mängel und teilte mit einem Rundschreiben den Fachbereichen und Instituten mit, dass ein paralleles Führen von Studentenakten, auch in Form von *Karteikarten mit Passfotos,* unzulässig ist und durch die Sekretariate lediglich eine Speicherung weniger Daten, wie Namen, Matrikelnummer, Lehrveranstaltung, Dozent und Benotung, zur Dokumentation der Studienleistung erforderlich ist.

Epidemiologie und Datenschutz – Eine Diskussion trug Früchte

Im Mai 1998 fand eine von zunehmendem gegenseitigem Verständnis geprägte Diskussion zwischen Vertretern der *Deutschen Forschungsgemeinschaft* und der Arbeitsgemeinschaft der wissenschaftlichen *medizinischen Fachgesellschaften* sowie der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ihren erfolgreichen Abschluss. Die Deutsche Arbeitsgemeinschaft für *Epidemiologie* und der Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes

und der Länder fassten einen gemeinsamen Beschluss[154]. Der Beschluss spiegelt den gegenwärtigen Stand der Diskussion und eine Reihe von Lösungsmöglichkeiten wieder[155]. Der Hessische Datenschutzbeauftragte stellte sein jährliches Datenschutzforum unter das Thema „Forschung und Datenschutz“[156], womit die Diskussion fortgesetzt wurde.

Da Epidemiologie und Datenschutz traditionell im Spannungsfeld des Schutzes der Persönlichkeitsrechte der von der Datenverarbeitung Betroffenen und dem wissenschaftlichen Anliegen an der Auswertung von *Gesundheitsdaten* stehen, wurden im Beschluss rechtliche *Rahmenbedingungen für die Forschung* definiert. Der Forscher hat zunächst zu prüfen, ob sein Forschungsziel durch die Nutzung vorhandener anonymisierter Daten, beispielsweise die der amtlichen Statistik, erreicht werden kann. Wenn dies nicht der Fall ist, können personenbezogene Daten auf freiwilliger Basis und mit Einwilligung der Betroffenen verarbeitet werden. Nur unter sehr engen Voraussetzungen, die vom Gesetzgeber festzulegen sind, und wenn es keine Alternativen gibt, die für die Betroffenen weniger belastend sind (z. B. Anonymisierungs- bzw. Pseudonymisierungsverfahren), kann es zulässig sein, ohne Einwilligung der Betroffenen Daten zu verarbeiten.

Die mit Lösungsansätzen im Weiteren bei Querschnittserhebungen, Kohortenstudien, retrospektiven Kohortenstudien, Fall-Kontroll-Studien diskutierten Fragestellungen sind folgende:

- Können die für einen bestimmten Zweck mit Einwilligung der Betroffenen oder auf anderer Grundlage einmal erhobenen Daten auch für die weitere Forschung, also die Bearbeitung neuer Fragestellungen, genutzt werden oder ist dies nur bei erneuter Einwilligung zulässig?
- Sind die Einzeldaten in jedem Fall nach Beendigung des Forschungsvorhabens zu löschen und gefährdet dies nicht die Nachprüfbarkeit der Forschungsergebnisse?
- Dürfen Einzeldaten aus verschiedenen Forschungsprojekten zusammengeführt und gemeinsam statistisch ausgewertet werden, insbesondere dann, wenn nur dadurch ausreichend große Fallzahlen erreicht werden können?
- Wie kann eine Einverständniserklärung so gestaltet werden, dass sie zum einen den Betroffenen ausreichend über die Tragweite seiner Einwilligung informiert und zum anderen die Forschung nicht behindert?

154 Anlagenband „Dokumente zum Datenschutz 1998“, Teil B II
155 JB 1996, 4.5.1 und JB 1997, 4.5.1
156 Hamm/Müller (Hrsg.), Datenschutz und Forschung, Baden-Baden 1999; im Internet http://www.hessm.de/ndsb

- Unter welchen Rahmenbedingungen dürfen Daten verschiedener Quellen personenbezogen verknüpft werden? Welche Rolle bei der Sicherung der Anonymität können dabei Treuhänder als vertrauenswürdige Dritte, die diese Verknüpfung ohne Interesse an der Forschung vornehmen, spielen?
- Welche Rahmenbedingungen müssen erfüllt sein, damit für wissenschaftliche Vorhaben nicht nur zusammengefasste Statistiken, sondern auch anonymisierte Einzeldaten der amtlichen Statistik unter Wahrung des Statistikgeheimnisses genutzt werden dürfen?
- Können statistische Einzelangaben dauerhaft archiviert werden, um einen unwiederbringlichen Verlust für die spätere wissenschaftliche Forschung zu vermeiden?
- Besteht die Möglichkeit, Krankheitsregister (wie z. B. die Krebsregister) zu nutzen, um mit Patienten einer bestimmten gesundheitlichen Exposition in Kontakt zu treten?

Da Studien häufig in mehreren Bundesländern oder bundesweit stattfinden, sind durch die Forscher unterschiedliche datenschutzrechtliche Regelungen zu berücksichtigen. Zur Vereinfachung des Verfahrens wurde vereinbart, dass der Studienleiter sich entweder an den für ihn zuständigen Datenschutzbeauftragten oder den Datenschutzbeauftragten wendet, in dessen Bundesland die zentrale Speicherung der Forschungsdaten erfolgen soll. Dieser wird dann die Stellungnahmen der anderen Datenschutzbeauftragten zu dem Projekt koordinieren.

Statistikgeheimnis wider die empirische Wirtschaftsforschung

Im Juni 1998 veröffentlichten Wirtschaftswissenschaftler ein Memorandum zu Erfolgsbedingungen *empirischer Wirtschaftsforschung* und empirisch gestützter wirtschafts- und sozialpolitischer Beratung. Neben dem Begehren der Wissenschaftler nach Zugang zu statistischen Daten, die außerhalb der amtlichen Statistik gesammelt werden (beispielsweise durch Bundesministerien, die Bundesbank oder die Bundesanstalt für Arbeit), möchten die Forscher einen unmittelbaren *Zugang zu den Einzeldaten der amtlichen Statistik* über Unternehmen erhalten. Das Memorandum gab der Diskussion zur Nutzung anonymisierter Einzeldaten der amtlichen Statistik neuen Aufschwung. So wurde beispielsweise vorgeschlagen, Wissenschaftler zeitweise als Mitarbeiter in die statistischen Ämter zu entsenden oder von diesen eine Vertiefung der Auswertung im Auftrag der Wissenschaft zu verlangen. Beide Wege sind problematisch, da sie entweder die Unabhängigkeit der Wissenschaft (Wissenschaftler als Mitarbeiter der statistischen Ämter) beschränken oder den Status der Ämter bezüglich ihrer Neutralität und Objektivität berühren würden. Daher gilt es, Möglichkeiten zu finden, die entweder den Wissenschaftlern faktisch oder total anonymisierte Einzeldatensätze zur Verfügung stellen oder dass durch die Statistik im Auftrag der

Wissenschaft noch nicht hinreichend anonymisierte Daten ausgewertet werden können, ohne dass die Wissenschaftler unmittelbar Zugriff auf die Einzeldaten haben (fremdrechnen).

Grundsätzlich abzulehnen ist auch aus datenschutzrechtlichen Erwägungen die geforderte *„Überprüfung" der einzelstatistischen Datensätze* hinsichtlich ihrer Wahrhaftigkeit und Richtigkeit durch die Wissenschaft. Dies würde der statistischen Geheimhaltung als konstitutives Element der amtlichen Statistik zuwiderlaufen und könnte die Akzeptanz für die Datenerhebungen bei den Betroffenen (Einwohner oder Wirtschaftsunternehmen) erheblich einschränken. Nur wenn die amtliche Statistik insbesondere bei ihren auf Auskunftspflicht beruhenden Datenerhebungen den Betroffenen rechtlich und verfahrenstechnisch abgesichert garantiert, dass die erhobenen Daten unter keinen Umständen mit einem auch noch so schwachen Personenbezug Dritten bereitgestellt werden, ist für diese die „Nachteilsfreiheit" und damit auch ein wesentliches Element der statistischen Geheimhaltung nachvollziehbar. Ohne die Sicherung der „Nachteilsfreiheit" für die Betroffenen würden statistische Ergebnisse schon bei der Erhebung verzerrt werden. Dies ist beispielsweise auch eine Schlussfolgerung aus der Deformation statistischer Erhebungen, wie sie bei politischer Einflussnahme in der DDR zu verzeichnen war.

Das Nierenbehandlungsregister QuaSi-Niere geht in Dauerbetrieb

Die Tragfähigkeit der für das *Nierenbehandlungsregister*[157] datenschutzrechtlichen Rahmenbedingungen sowie der technischen und organisatorischen Lösungen wird sich ab 1999 neu erweisen müssen. Bislang war das Register als öffentliche Stelle bei der Ärztekammer Berlin angebunden und wurde überwiegend vom Bundesministerium für Gesundheit finanziert. Für dieses Register gibt es nicht wie beispielsweise beim Krebsregister eine für alle Beteiligten bindende Rechtsvorschrift bzw. einen Staatsvertrag, sondern eine auf Konsens beruhende Kooperation der Spitzenverbände der Krankenkassen, Dialyseleistungserbringer und Patientenvertreter. Die Beteiligten haben sich darauf geeinigt, *QuaSi-Niere* als gemeinnützige GmbH weiterzuführen und zu finanzieren. Damit ist die Kontinuität des Registers gesichert. Die vorliegenden Einwilligungserklärungen der Patienten zur Speicherung und Anonymisierung ihrer Gesundheitsdaten bei QuaSi-Niere bzw. dem Datentreuhänder können nur dann als Grundlage für die Datenverarbeitung herangezogen werden, wenn der datenschutzrechtliche Standard sich nicht verschlechtert. Dies wurde durch Verträge gesichert, in denen sich die QuaSi-Niere GmbH auch dem Berliner Datenschutzgesetz und der Kontrolle durch den Berliner Datenschutzbeauftragten

[157] JB 1997, 4.4.2

unterworfen hat, um keine Reduzierung der Patientenrechte durch den *Wechsel der Trägerschaft* von einer öffentlichen Stelle des Landes Berlin in eine private Stelle im Anwendungsbezirk des Bundesdatenschutzgesetzes zuzulassen.

Beispielhaftes aus der Forschung – aber auch etwas Bedenkliches

Weiterhin rege nutzen Wissenschaftler die Möglichkeit, sich vor Beginn ihrer Projekte beraten zu lassen.

> *Im Rahmen einer „Public Health Studie" soll in einem Berliner Bezirk bei allen Schülern eines bestimmten Jahrganges über einen längeren Zeitraum die Häufigkeit von Zahnunfällen untersucht werden. Dabei sollen anlässlich der jugendzahnärztlichen Untersuchungen in den Schulen Daten erhoben werden.*

Für die erste Phase empfahlen wir durch den *zahnärztlichen Dienst* auf den Erhebungsbögen gesondert zu signieren, ob die Zähne der Kinder Unfallspuren aufweisen. Diese Daten werden dann zu statistischen Tabellen zusammengefasst, so dass einer Übermittlung dieser so anonymisierten Daten datenschutzrechtlich nichts entgegen steht. Bei der nächsten zahnärztlichen Untersuchung im danach folgenden Schuljahr soll den Kindern, bei denen eine neue unfallbedingte Zahnverletzung erkennbar ist, von den Jugendzahnärzten ein Elternbrief und ein Fragebogen übergeben werden, mit dem die Eltern dann freiwillig zu den Wissenschaftlern Kontakt aufnehmen können.

Das *Deutsche Zentralregister für kindliche Hörstörungen* (DZH) mit Standort am Universitätsklinikum Benjamin Franklin der Freien Universität Berlin ist inzwischen fest etabliert[158].

Meldungen erfolgen zur Zeit von 83 Einrichtungen. Gut 2 500 Patientendatensätze wurden bis heute aufgenommen, monatlich kommen gegenwärtig ca. 100 neue dazu.

Da es sich um ein Register Minderjähriger handelt, werden die Patienten bei Erreichen der Volljährigkeit angeschrieben und um ihr Einverständnis zum Verbleib der Daten im DZH gebeten. Bei Ablehnung der weiteren Registrierung im DZH werden die Datensätze gelöscht. Sind Betroffene (z. B. wegen Umzugs) nicht mehr auffindbar, werden deren Datensätze aus dem Gesamtregister herausgenommen, gesondert gesichert gespeichert und nach weiteren ergebnislosen Anschreiben ebenfalls vernichtet.

In den Sommermonaten befragten die *Berliner Verkehrsbetriebe* rund 110 000 Personen in Berlin und im Brandenburger Umland. Die Adressen wurden nach einem Zufallsverfahren aus den Datenbeständen der

[158] JB 1994, 4.15

Melderegister Berlins bzw. der Umlandverwaltungen ausgewählt. Zurückzusendende Fragebögen enthielten keine Namen, sondern lediglich eine Nummer. Natürlich war die Befragung freiwillig. Um jedoch eine hohe Repräsentativität der Ergebnisse zu erreichen, wurden nach einer gewissen Frist diejenigen, die nicht geantwortet hatten, nochmals um ihre Teilnahme gebeten. Hierfür wurde die Adresse nochmals aktiviert.

Leider sorgte eine andere ebenfalls von den Berliner Verkehrsbetrieben in Auftrag gegebene Befragung für eine gewisse Verwirrung. Im Unterschied zur großen Verkehrsbefragung, die postalisch durchgeführt und worüber auch ausführlich in der Presse berichtet wurde, erfolgte die zweite Datenerhebung durch Interviewer. Dies verwirrte Betroffene, die hier „Trittbrettfahrer" vermuteten, die nicht selten parallel zu großen, auch von der Allgemeinheit akzeptierten freiwilligen Datenerhebungen für mitunter dubiose Zwecke Daten sammeln.

Die BVG teilte uns mit, dass künftig eine zeitliche Nähe von verschiedenen Befragungen vermieden wird.

„Beeinflusst intensive Musikerziehung die Entwicklung von Kindern?"

Diese Frage versuchte eine Forschergruppe des Instituts für Begabtenforschung und Begabtenförderung in der Musik an der Universität Paderborn zu beantworten. Über die gesamte sechsjährige Grundschulzeit seit 1992 wurden 170 Kinder in musikbetonten und anderen Schulen befragt. Anfangs hielten wir es für undurchführbar, über diesen langen Zeitraum hinweg je Kind weit mehr als 10 000 verschiedene Merkmale (von der Messung des Intelligenzquotienten bis zu Musikalitätstests) zu erheben.

Ein Problem war die *Akzeptanz der Eltern* der Kontrollgruppen aus den nicht-musischen Schulen, die damit rechnen mussten, dass das Ergebnis der Untersuchung lauten könnte, dass durch die Schulwahl der Eltern die geistige, emotionale und soziale Entwicklung ihrer Kinder nicht so weit ist wie bei den anderen Kindern. Es wurde vereinbart, dass die beiden das Projekt leitenden Wissenschaftler die Datenerhebungen in Berlin selbst durchführten und diese nicht-wechselnden Assistenten überließen. Die Eltern jedes Schülers sollten halbjährlich eine auf das Kind bezogene Zusammenfassung der bisherigen Ergebnisse erhalten und die Möglichkeit haben, in einer individuellen Sprechstunde Fragen zu stellen. Die Daten waren selbstverständlich codiert und wurden dem Lehrer nicht zur Kenntnis gegeben. Somit war für alle Kinder und deren Eltern trotz dieser zusätzlichen Informationen über die Entwicklung der Kinder eine Gleichbehandlung gesichert. Unter diesen Bedingungen, die die Forscher vor Beginn der Datenerhebung auf Elternabenden vorstellten, waren die Erziehungsberechtigten gern zu einer Einwilligung bereit. In den Klassenstufen 1 bis 4 nahmen jeweils fast alle der Eltern die „wissenschaftliche Elternsprechstunde" in

Anspruch. Auch in den nachfolgenden Schuljahren wurde dieses Angebot noch von weit mehr als 50 % genutzt. Im Juni 1998 wurde das Projekt im Freizeit- und Erholungszentrum (FEZ) in der Wuhlheide mit einem Abschiedsfest beendet. In den verschiedenen, nicht nur musikalischen Programmteilen nahmen die Schüler die „Gewohnheiten" der Wissenschaftler durch verschiedene Sketche humorvoll aufs Korn. Für die Akzeptanz der Studie sprachen auch verschiedene Anfragen von Eltern, ob es möglich wäre, diese Studie weiterzuführen, indem über die beteiligten Kinder noch Daten aus der Sekundarstufe nacherhoben werden würden.

Unbesungene Helden

Einem diffizilen Kapitel der Deutschen Geschichte nähert sich das Zentrum für Antisemitismusforschung der Technischen Universität Berlin mit ihrem Forschungsprojekt „Rettung von Juden im nationalsozialistischen Deutschland". Es soll untersucht werden, unter welchen Umständen und mit welchen Motiven es gelang, in Berlin etwa 1 500 Juden vor der Deportation und der Ermordung zu retten. Alle noch bekannten Fälle der Rettung von Juden in Deutschland sollen in einer Datenbank zusammengetragen werden. Dies betrifft nicht nur die geehrten und entschädigten Deutschen, die so genannten „Unbesungenen Helden", sondern auch Personen, die von den Geretteten Geld oder andere Gegenleistungen nahmen, selbst die, die als Schmuggler tätig waren oder die Versteckten sexuell oder als Arbeitskräfte ausbeuteten.

Auch wenn der überwiegende Teil der Geretteten wie auch der Retter heute nicht mehr am Leben ist, gilt es, deren auch nach dem Tode nachwirkende Persönlichkeitsrechte sowie die Persönlichkeitsrechte der Kinder und anderer Verwandten zu wahren. Dies erfolgt durch technische und organisatorische Maßnahmen, die einen datenschutzgerechten Umgang mit den über 1 500 Akten der Entschädigungsbehörde und den 600 Akten der Innenverwaltung der zur Ehrung vorgeschlagenen „Unbesungenen Helden" sichergestellt. Nach Abschluss der Forschung werden die Akten zur weiteren Aufbewahrung an das Landesarchiv übergeben.

Bedenkliches . . .

Anfang des Jahres 1995 wurde ein Berliner Wissenschaftler mit einer Studie zu einer bestimmten Erkrankung beauftragt. Über verschiedene Ärzte wurden bundesweit Personen angeschrieben, deren bisherige Befunde für das Vorliegen der zu untersuchenden Krankheit sprachen. Den Probanden wurde versprochen, sämtliche Befunde und Ergebnisse mit ihnen und den behandelnden Hausärzten ausführlich zu besprechen. Als nach einer ersten internen Vorstellung der Testergebnisse und einer nachfolgenden Presseerklärung Zweifel an der Solidität der durchgeführten Studie sowohl bei Berufskollegen als auch bei den Pro-

banden aufkam, widersprachen einige Probanden der weiteren Auswertung ihrer Daten, also auch einer weiteren anonymisierten Auswertung der Testergebnisse, und baten um die Herausgabe von Kopien der Einzelbefunde und Tests. Da dies mit einer erheblichen Verzögerung und zunächst nicht vollständig erfolgte, wurden wir Ende des Jahres 1997 um Unterstützung gebeten.

Die Verweigerung der Herausgabe von Befunden einschließlich der Testprotokolle durchgeführter Untersuchungen entbehrt jeglicher Rechtsgrundlage.

Uns wurde zugesichert, dass den Probanden auch Kopien der sie betreffenden Unterlagen übersandt werden. Diese waren zunächst mit den Unterlagen anderer Probanden verwechselt worden. Aus diesem Fall lassen sich Schlussfolgerungen für künftige Studien ziehen. Wissenschaftliche Untersuchungen, insbesondere wenn sie wie diese mit einem Krankenhausaufenthalt verbunden sind, sollten zunächst durch eine umfassende Information und die Zusicherung von Rechten und einzuhaltender Pflichten um die Einwilligung der Probanden werben. Die *informierte schriftliche Einwilligung,* die den Zweck der Studie, die durchzuführenden Untersuchungen, die Nutzung und Übermittlung der Ergebnisse sowie die Veröffentlichung umfassend vorschreibt, ist unerlässlich. Sie stellt zudem sicher, dass auch bei möglichen Zweifeln die wissenschaftlichen Ergebnisse sachlich diskutiert werden können. Unsere Erfahrungen bestätigen, dass es von den Probanden honoriert wird, wenn der die Studie leitende Wissenschaftler mit ihnen persönlich in Kontakt tritt und dessen kontrollierende Einflussnahme spürbar ist.

. . . und Nachahmenswertes

Im März 1998 gab die Medizinische Fakultät der Albert-Ludwigs-Universität Freiburg Empfehlungen der Kommission „Verantwortung in der Forschung“ heraus, in denen die Verantwortung der Wissenschaftler sowohl bezüglich ihrer wissenschaftlichen Ergebnisse als auch gegenüber den Probanden dargelegt werden. *Selbstverpflichtungen der wissenschaftlich Forschenden* dürften künftig an Bedeutung gewinnen und damit die Akzeptanz der Forschung wesentlich erhöhen.

4.5.2 Schule

Integration von Kindern mit sonderpädagogischem Förderbedarf

In der Stellungnahme zum Jahresbericht 1996 teilte der Senat mit, dass an einer *Rechtsverordnung zur sonderpädagogischen Förderung* (FörderVO), in der datenschutzsichernde Regelungen integraler Bestandteil sein werden, gearbeitet wird[159]. Obwohl wir bereits im Jahresbericht 1995[160] eine derartige Regelung angemahnt haben, erhielten wir erst Ende des Jahres 1998 von einem Verordnungsentwurf Kenntnis. Dieser Verordnungsentwurf ist nicht unproblematisch, da er durch die Gliederung der Förderschwerpunkte und Ziele der sonderpädagogischen Förderung eine *„Katalogisierung“ der zu fördernden Schüler* mit sich bringen könnte. Als Förderschwerpunkte, die jeweils gesondert behandelt werden, sind bezeichnet: Sehen, Hören, körperliche und motorische Entwicklung, Sprache, Lernen, geistige Entwicklung sowie emotionale und soziale Entwicklung (Verhalten). Wir haben uns bereit erklärt, an einer Lösung mitzuarbeiten, die ein schematisches, die Persönlichkeitsrechte verletzendes Vorgehen ausschließt. Die datenschutzrechtlichen Regelungen im Verordnungsentwurf wie beispielsweise über die Schulwegbeförderung von Kindern mit Behinderungen bilden zusammen mit der Schuldatenverordnung einen zusammenhängenden und gut ausgestalteten Komplex.

Zu begrüßen ist, dass das Landesschulamt im Vorgriff auf die Förderverordnung verbindlich einheitliche Formulare für die sonderpädagogischen Förderbögen und das Förderausschussverfahren vorschreibt.

Datenschutz im Internat – eine Lösung in Sicht

Nachdem wir[161] in einem Internat erhebliche datenschutzrechtliche Mängel vorfanden und diese zweimal beanstandeten, begann die Senatsschulverwaltung mit Arbeiten an einer *Musterinternatsordnung.* Wir boten unsere Beratung an und machten Vorschläge für einen Internatsvertrag und eine *Haus- und eine Internatsordnung.* Nach Diskussion dieser Entwürfe unter den Internatsleitern wurden mit Beginn des Schuljahres 1998/99 für die unmittelbar dem Landesschulamt unterstellten Berliner Schulinternate diese Musterunterlagen vorläufig für verbindlich erklärt.

Ab 1999 – endlich ein einheitlicher Fragebogen für die Einschulungsuntersuchungen

Während der Jahresbericht 1997[162] erschien, wurden in Berlin die Einschulungsuntersuchungen durch die Jugendgesundheitsdienste der Bezirke durchgeführt. Trotz einiger Korrekturen an den Erhebungsbögen wurden nach wie vor von den 23 Bezirken fünf verschiedene Fragebögen genutzt. Insbesondere die *Verknüpfung von Schulreifeuntersuchung und Gesundheitsberichterstattung,* die für die Eltern kaum erkennbar war, führte wiederum zu einer Reihe von Anfragen und Beschwerden. Im Herbst 1998 einigten sich die Jugendgesundheitsdienste der

159 Abghs.-Drs. 13/1721

160 5.9
161 JB 1996, 4.5.2
162 JB 1997, 4.5.2

Bezirke auf einen einheitlichen Erhebungsbogen und ein Anschreiben, das die Eltern auf die unterschiedlichen Verwendungszwecke der Daten und die Freiwilligkeit bezüglich der ausschließlich für die Gesundheitsberichterstattung und nicht für die Einschulungsuntersuchung benötigten Angaben hinweist und sie um ihre schriftliche Einwilligung bittet.

4.5.3 Statistik

Volkszählung 2001 – Ein Methodenwechsel oder eine Notlösung?

Bundesweit rangen die amtlichen Statistiker im vergangenen Jahr um eine Lösung für die Anforderungen der EU an einen *gemeinschaftsweiten Zensus* im Jahre 2001. Im August 1998 wurde der Bericht einer Arbeitsgruppe von Bund und Ländern vorgelegt. Es galt, einem Auftrag der Innenministerkonferenz entsprechend, Modelle für einen rechnergestützten Zensus zu entwickeln, der einen Paradigmenwechsel von einer primärstatistischen Totalerhebung (unmittelbare Befragung der Bevölkerung) zu einem registergestützten System ermöglichen soll. Wichtigstes Ergebnis ist, dass ein auf den Melderegistern und anderen vorhandenen Datenbeständen aufsetzender Zensus noch nicht mit einer herkömmlichen Volkszählung vergleichbare und inhaltlich gleichwertige Ergebnisse liefern wird.

Im Jahresbericht 1997[163] erläuterten wir die beiden unterschiedlichen als Bundes- bzw. Ländermodell bezeichneten Ansätze. Wichtigster Unterschied ist, dass beim Bundesmodell verschiedene Datenbestände, wie die Melderegister oder die Beschäftigtendatei der Bundesanstalt für Arbeit, ergänzt um den Mikrozensus, nebeneinander ausgewertet und nicht personenbezogen verknüpft werden. Im Unterschied dazu ist beim Ländermodell eine personenbezogene Zusammenführung von Einzeldatensätzen zu einer Volkszählungsdatei vorgesehen. Das Ländermodell soll einen Grundstock für den Aufbau kommunaler Gebäude- und Wohnungsregister bilden, die dann wiederum durch eine Verknüpfung mit anderen Registern wie dem Melderegister den Einstieg in eine permanente *Registerstatistik* sowohl auf der Ebene des Bundes und der Länder als auch der Kommunen erlauben würden.

Beide Modelle bringen zwar eine geringere Belastung der Bürger durch die nicht in jedem Fall notwendige Befragung mit sich, verlangen jedoch eine erhebliche Akzeptanz und auch eine Auskunftspflicht für jeden. So ist es beispielsweise erforderlich, dass bei der Überprüfung von Mehrfachfällen (z. B. Doppelungen in den Melderegistern bei fehlender Abmeldung) sowie bei Differenzen zwischen der Gebäude- und Wohnungszählung und den Melderegistern (bewohnte Adressen) die betroffenen Personen angesprochen werden müssen. Eine Akzeptanz der Betroffenen ist hier nur zu erwarten, wenn transparent gemacht

163 4.5.3

wird, dass es sich ausschließlich um statistische Feststellungen, ohne Nachteile oder Konsequenzen für den einzelnen Einwohner, handelt. Mit der Durchführung eines solchen Zensus wird also der Inhalt der *Melderegister* nicht verändert; Korrekturen erfolgen nur in den ausschließlich für statistische Zwecke zusammengeführten Dateien der statistischen Landesämter und des Statistischen Bundesamtes. Für welches Modell auch immer sich der Bundesgesetzgeber in den nächsten Monaten entscheiden wird, die Diskussion über die Nutzung von Verwaltungsregistern für statistische Zwecke und ihre mögliche Zusammenführung zu Statistikregistern ist noch lange nicht abgeschlossen. Aus datenschutzrechtlicher Sicht sollten Wege gefunden und erprobt werden, bei denen Erfahrungen der vergangenen Jahre mit der Pseudonymisierung von Angaben sowie Datentreuhändermodellen berücksichtigt werden. So könnte beispielsweise der Gesetzgeber zunächst für den Zensus 2001 eine einfache Variante bundesweit vorschreiben, zugleich aber punktuell und stichprobenhaft neue Methoden, wie sie im Ländermodell vorgeschlagen werden, erproben lassen.

Durch die Vorgabe, einen registergestützten Zensus durchzuführen, werden allerdings die Grundsätze der Neutralität, Objektivität und wissenschaftlichen Unabhängigkeit der Amtlichen Statistik erheblich berührt. Es besteht nach wie vor die Gefahr, dass mit dem Zensus 2001 Verfahren gewählt werden, die nicht zu einem geeigneten Ergebnis führen können. Damit wäre der Eingriff in das Recht auf informationelle Selbstbestimmung nicht verhältnismäßig, so dass eine derartige Erhebung datenschutzrechtlich als unzulässig anzusehen wäre.

Bei der *Zusammenführung von Einzeldatensätzen,* wie sie im Ländermodell vorgesehen sind, könnte die Eingriffstiefe durch eine *Pseudonymisierung* wesentlich abgemildert werden. Dies könnte dadurch geschehen, dass die Erhebungsmerkmale der zu verknüpfenden Einzeldatensätze erst verarbeitet werden, wenn durch den Abgleich der Hilfsmerkmale eine 1:1-Zuordnung erfolgt ist und die Hilfsmerkmale getrennt gespeichert und verarbeitet werden. Aus den Hilfsmerkmalen könnte ein Pseudonym erzeugt werden, mit dem es möglich wäre, wiederum die Einzeldatensätze der Erhebungsmerkmale ohne die unmittelbar auf die Person zeigenden Hilfsmerkmale zu verknüpfen.

Erhebungen für DIE Statistik?

Immer wieder begegnen uns bei Prüfungen oder im Zusammenhang mit Eingaben Datenerhebungen, die angeblich für „DIE Statistik" erforderlich seien. Manchmal kann kaum jemand in den geprüften Behörden erläutern, auf welcher Rechtsgrundlage von ihnen nichtanonymisierte und damit personenbezogene Daten erhoben und an eine Aufsicht führende Behörde übermittelt werden. Gemeinsam ist diesen Datenerhebungen, dass der Empfänger dieser Daten nicht das Statistische

Landesamt ist. Mitunter wird noch darauf verwiesen, dass es sich um eine Geschäftsstatistik oder eine Statistik im Verwaltungsvollzug handele.

Das System der *amtlichen Statistik* umfasst EG-Statistiken, Bundesstatistiken, Landesstatistiken sowie Statistiken im Verwaltungsvollzug. Nach heute üblichen Definitionen ist Statistik der Inbegriff aller Methoden zur Gewinnung und Analyse empirischer Daten. Mit einer Statistik werden keine Aussagen über einzelne Individuen, sondern über Gesamtheiten (Kollektive) gemacht. Diesen Aussagen liegt ein theoretisch fundiertes Modell zugrunde, das dynamisch auf Veränderungen bei „Massenerscheinungen" reagiert und angepasst wird. Ziel ist es, quantitative und qualitative Veränderungen von „Massenerscheinungen" abzubilden. Die Statistik darf nicht auf die Identifizierung der Einzelerscheinung (einschließlich der einzelnen Person) gerichtet sein. Eine Zweckbindung bei der Verwendung dieser Daten gibt es nicht. Die Statistik produziert „Zahlen für alle". Dies ist verfassungsrechtlich nur hinnehmbar, wenn die die Statistik aufbereitende Stelle besondere Vorkehrungen zur *Wahrung des Statistikgeheimnisses* trifft. Dies wird sowohl durch die Abschottung der Statistikstelle nach außen als auch durch die frühstmögliche Anonymisierung gesichert. Die Unterscheidung nach Erhebungs- und Hilfsmerkmalen erlaubt die frühstmögliche Anonymisierung über die Vernichtung der Hilfsmerkmale.

Erhebungsmerkmale sind die Angaben über persönliche und sachliche Verhältnisse, die für die statistische Auswertung bestimmend sind. Dies können qualitative Merkmale, wie beispielsweise männlich oder weiblich, oder quantitative Merkmale, wie die Anzahl der Beschäftigten eines Unternehmens, sein.

Hilfsmerkmale hingegen dienen der technischen Durchführung der einzelnen Statistik. Sie werden lediglich für die Aufbereitung benötigt, um die Plausibilität durch Rückfragen beim Betroffenen oder bei der Stelle zu ermöglichen, die die Daten über die Betroffenen speichert (Sekundärstatistiken). Danach sind diese Hilfsmerkmale nicht mehr erforderlich und können von den anderen Daten getrennt und dann gelöscht werden. Häufig ist auch dann noch eine Deanonymisierung möglich. Um dies zu verhindern, sind die Statistikstellen nach außen hin abgeschottet und Empfänger der Statistiken erhalten nur zusammengefasste Daten, die keinen Rückschluss auf das Individuum mehr erlauben.

Etwas anders verhält es sich bei den *Statistiken im Verwaltungsvollzug*. Nach dem Landesstatistikgesetz[164] sind Statistiken im Verwaltungsvollzug Statistiken, die durch die Aufbereitung von Daten entstehen, die aufgrund nichtstatistischer Rechts- oder Verwaltungsvorschriften oder auf sonstige Weise bei den Verwaltungsstellen Berlins anfallen. Dazu gehören Geschäfts- und Registerstatistiken.

[164] § 2 Abs. 1 Ziff. 4 LStatG, GVBl. 1992, S. 365

Geschäftsstatistiken liegen dann vor, wenn sich die statistische Bearbeitung der Daten zweckmäßigerweise nicht vom Geschäftsgang trennen lässt. Von *Registerstatistiken* wird gesprochen, wenn die Daten in automatisierten Verwaltungsregistern oder Dateien enthalten sind.

Für diese Statistiken ist nach dem Landesstatistikgesetz die Verwaltung zuständig, bei der die Daten des Verwaltungsvollzugs anfallen oder vorliegen. Statistiken im Verwaltungsvollzug dienen in erster Linie der Dokumentation des Umfangs der eigenen Tätigkeit der Verwaltungsstelle und damit eigenen (Planungs-)Zwecken. Zumeist sind sie Fallauszählungen. Nach Abschluss eines Vorganges wird z. B. auf einem gesonderten Blatt unter der Rubrik „Abgeschlossene Vorgänge" ein Strich gemacht und am Monatsende die Anzahl der abgeschlossenen Vorgänge zusammengezählt. Die gewonnene Zahl erlaubt Nutzern der Statistik keinen Rückbezug auf den einzelnen bearbeiteten Vorgang.

Mit einer Statistik nichts zu tun hat die *Erhebung personenbeziehbarer Einzeldatensätze*. Die Hilfsmerkmale, wie der Name und das Aktenzeichen, die der Identifizierung des Individuums bzw. des Einzelvorganges dienen, sind für eine statistische Aufbereitung nicht erforderlich und damit nicht in die Statistik aufzunehmen. Eine z. B. als „Eingangsstatistik" bezeichnete personenbezogene Liste aller eingegangenen Anträge stellt keine Statistik dar. Es handelt sich damit um keine statistische Auszählung von Fallzahlen. Bei der Weitergabe derartiger Listen würden personenbezogene Daten unzulässig übermittelt werden[165].

Der Landesgesetzgeber hat lediglich in einem Ausnahmefall zugelassen, dass personenbezogene Datensätze zum Zwecke der Erstellung einer Statistik im Verwaltungsvollzug übermittelt werden. Das Statistische Landesamt darf im Auftrag anderer Behörden nichtanonymisierte Einzeldaten zur Erstellung einer Statistik im Verwaltungsvollzug erhalten und verarbeiten. Herr der Daten bleibt jedoch, im Unterschied zu einer Bundes- oder Landesstatistik, die jeweilige Verwaltung. Das Statistische Landesamt darf nur im Rahmen der Anordnung der auftraggebenden Stellen der Verwaltung und mit den von ihr zur Verfügung gestellten Daten Aufbereitungen durchführen und statistische Ergebnisse veröffentlichen. Ein Beispiel ist die polizeiliche Kriminalitätsstatistik.

4.6 Wirtschaft

4.6.1 Banken und Versicherungen

Keine Werbung mit öffentlichen Daten

In einer flächendeckenden Aktion schrieb die Investitionsbank Berlin (IBB) gezielt Darlehensnehmer von Hypothekenbanken und anderen Banken an, bei denen eine Prolongation des Darlehens unmittelbar

[165] vgl. 4.2.2

bevorstand. Dabei bot die IBB eine Umfinanzierung der restlichen Darlehenssumme an. Die IBB benutzte hierzu die Daten, die sie aufgrund ihrer öffentlich-rechtlichen Sonderstellung erlangt hat, um sich anschließend Wettbewerbsvorteile gegenüber anderen Banken zu sichern.

Zu den Aufgaben der IBB gehört die Unterstützung des Landes Berlin bei der Erfüllung öffentlicher Aufgaben. Sie fördert u. a. Maßnahmen auf den Gebieten des Wohnungs- und Städtebaus. In Erfüllung dieser öffentlichen Aufgabe ist die Investitionsbank Berlin *Bewilligungsbehörde für Bürgschaftsübernahmen* bei I b-Darlehen. In Wahrnehmung dieser Aufgabe verfügt die IBB über persönliche Daten der Kreditnehmer. Außerdem ist sie aufgrund der Datenbestände in der Lage, Einblick in die Kreditunterlagen der Förderdarlehen zu nehmen. Da sie die Daten aufgrund ihrer öffentlich-rechtlichen Sonderstellung erhalten hat, ist ihr Verhalten an den Vorgaben des Berliner Datenschutzgesetzes zu messen. Die zum Zweck der Bewilligung erhobenen Daten unterliegen der Zweckbindung des § 11 Abs. 1 und 2 BlnDSG. Danach dürfen personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie erhoben oder gespeichert worden sind. Dies schließt eine Verwendung der Daten zu Werbezwecken aus.

Nach Darstellung der IBB besteht der Zweck der Darlehensangebote darin, Mieterhöhungen und Subventionszahlungen zu vermeiden, soweit sie auf überhöhte Konditionen der zur Finanzierung des Bauvorhabens aufgenommenen Darlehen beruhen. Die Angebote könnten als Verhandlungsgrundlage für das Prolongationsgespräch bei den Hausbanken genutzt werden. Wir haben der IBB empfohlen, überhöhte Darlehensabschlüsse dadurch zu vermeiden, dass den Förderungsnehmern vor einer Prolongation der marktübliche Kapitalzins mitgeteilt wird, ohne selbst ein Angebot zu unterbreiten. Mit der bloßen Information würde die IBB ihrer rechtlichen Aufgabe entsprechen. Die IBB hat unseren Vorschlag inzwischen aufgegriffen.

Adressänderung eines Bankkunden

Eine Bürgerin beschwerte sich bei uns, weil sie von der Landesbank Berlin (LBB) Kontounterlagen einer Kundin erhalten hatte. Beide wohnten in derselben Straße und hatten denselben Vor- und Nachnamen. Die Nichtkundin informierte umgehend die Landesbank über den aufgetretenen Fehler. Trotz dieser Information und trotz mehrerer weiterer Proteste der falsch Angeschriebenen erhielt sie weiterhin mehrere Wochen lang Kontoauszüge und Einladungen zu Aktionärstreffen ihrer Namensvetterin.

Etwa 10 % der Kunden der LBB ändern jährlich ihre Adresse. Sofern der Kunde die Änderung nicht mitteilt, erhält dieser die Sendungen von der Deutschen Post AG zurück. Diese ist meist mit einer neuen Versandadresse versehen. Die Landesbank nutzt die von der Post angegebene Adresse für die erneute Zustellung der Postsendung. In der Regel sind die *Adressangaben der Deutschen Post AG* zutreffend. Leider kommt es – wie sich hier herausstellte – bei der Post bei der Angabe der Adresse auch zu Fehlern und Verwechslungen.

Die Landesbank rechtfertigte ihr Verhalten damit, man habe erst über das Landeseinwohneramt (LEA) die richtige Adresse der Kundin ermitteln müssen. Da das LEA die Anfrage erst nach einigen Wochen beantwortet habe, habe man bis dahin die Kontounterlagen weiterhin an die Nichtkundin übersandt.

Im Fall einer falschen Adressierung muss bis zur genauen Ermittlung der Anschrift ein Postverbot für das betroffene Konto ausgesprochen werden. Sollte sich herausstellen, dass bei der Adressermittlung der Post häufiger Fehler vorkommen, sollte man zukünftig in dem ersten Schreiben an die neue Adresse keine Kontodaten übermitteln, sondern nur den Kunden bitten, die Richtigkeit der neuen Anschrift zu bestätigen.

Geldausgabeautomat und Bankgeheimnis

Ein Petent hatte versucht, an einem Geldausgabeautomaten (GAA), der nicht zu seinem kontoführenden Geldinstitut gehörte, mit Hilfe seiner ec-Karte die Auszahlung von Bargeld zu erhalten. Auf dem Display des GAA wurde ihm dies sinngemäß mit dem Hinweis „Auszahlung zurzeit nicht möglich“ verweigert. Eine technische Störung vermutend, startete er einen zweiten Versuch bei einer anderen Bank mit dem gleichen Ergebnis. Hartnäckig versuchte er es bei einem dritten Institut. Ein geldbringender Erfolg war ihm zwar nicht beschieden, jedoch erhielt er diesmal die – wiederum sinngemäße – Mitteilung „Limit überschritten“. Wäre ihm diese Nachricht an einem GAA seiner Bank übermittelt worden, hätte es ihn nicht überrascht, so jedoch vermutete er eine Verletzung des Bankgeheimnisses, da eine solche Information einer fremden Bank nicht zustünde.

Mit Beginn des Jahres 1998 wurden alle GAA-Transaktionen der Hausbank des Petenten auf *Online-Betrieb* umgestellt. Die von einem Bankkunden an einem institutsfremden GAA angestoßene Verfügung wird an die zur kontoführenden Bank gehörende *Authentisierungs-Zentrale* weitergeleitet. Von dort wird die Auszahlungsanforderung an das Bankrechenzentrum weitergegeben, wo das Kundenkonto überprüft wird. Ist eine Auszahlung – aus welchen Gründen auch immer – nicht möglich, übergibt der Bankrechner einen Code an den GAA der anderen Bank weiter, in dem er in einen Klartext umgewandelt und am Display angezeigt wird. Für die Umwandlung des Codes in den von Kunden zu lesenden Text gibt zwar der Zentrale Kreditausschuss (ZKA) Empfehlungen, die diesem Gremium angeschlossenen Geldinstitute sind jedoch nicht an einen allgemein verbindlichen Text gebunden. Daher bekam unser Petent verschiedene Hinweise bei seinen Ver-

suchen Geld abzuheben. Zu keinem Zeitpunkt werden Informationen über das Konto der Hausbank im GAA-Rechner der anderen Bank gespeichert. Dieser setzt lediglich auf der Grundlage des übermittelten Codes den Text um oder führt die Auszahlung durch und bildet dazu einen Datensatz für die Abrechnung der Transaktionsgebühren. Eine Protokollierung und Auswertung von Verfügungen findet dort nicht statt.

Fehlgeleitete Faxe

Irritiert beschwerten sich mehrere Bürger bei uns, die fehlgeleitete Fax-Nachrichten von verschiedenen Banken erhielten. Sie reichten von äußerst sensiblen Angaben über Bankkunden bis zu Personalunterlagen. So gingen Bonitätsanfragen für Kreditprüfungen, Angaben über Kontostände und Bewerbungsunterlagen bei den überraschten Bürgern ein. In einigen Fällen versuchten die Bürger, den ständigen Eingang von bankinternen Faxsendungen zu stoppen. Hinweise an die Kreditinstitute blieben aber erfolglos.

Als Hauptgrund für diese Fehlleitungen erwiesen sich Fehler beim Wählvorgang, die bei größerer Sorgfalt hätten vermieden werden können. Die Faxgeräte zeigen zwar an, welche Nummer angewählt wurde, bevor die Verbindung zustande kommt. Wenn aber diese Anzeige dem Absendenden entgeht und er nicht erkennt, dass die Nummer falsch ist, erfolgt die Übertragung ungehindert und vollständig. Bei der Übermittlung von Telefaxen ist die angewählte und im Display des Faxgerätes angezeigte Rufnummer vor dem Absenden nochmals genauestens zu kontrollieren. Im Gegensatz zum Telefonat, bei dem der Anrufende zumeist unmittelbar feststellen kann, falsch verbunden zu sein, sind andernfalls beim Fax die möglicherweise vertraulichen Daten sehr schnell auf dem unwiderruflich falschen Weg[166].

Bankdaten für Passanten

Eine Bürgerin traute ihren Augen nicht, als sie an einer Bank vorbeiging und von außen die Bildschirminhalte mehrerer Arbeitsplätze einsehen konnte. Die vertraulichen personenbezogenen Daten, die nur für den internen Geschäftsbetrieb gedacht waren und dem Bankgeheimnis unterliegen, konnten von vorbeigehenden Personen eingesehen werden.

Die Bank hatte vor kurzem Umbauarbeiten durchgeführt. Die Jalousien, die den Einblick auf die Monitore verhindern sollen, waren noch nicht geliefert. Um diesen Mangel unverzüglich zu unterbinden, haben wir umgehend eine Prüfung vorgenommen. Schon bei unserem Eintreffen wurden mehrere interessierte Personen vor dem Fenster angetroffen. Die betroffenen Monitore wurden sofort ausgeschaltet. Unsere Stichproben ergaben, dass die Monitore erst wieder in Betrieb genommen wurden, nachdem die Jalousien angebracht waren.

[166] vgl. JB 1994, 3.5 und die Empfehlungen des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten zu Datenschutz und Telefax

Fehladressierter Versicherungsnachtrag

Ein Bürger wendete sich an uns, der von einer Versicherung einen Nachtrag zum Versicherungsschein zugesandt bekommen hatte, obwohl er weder Kunde der Versicherung noch Halter des in dem Schein genannten Fahrzeuges war. Auch die darin angegebene Bankverbindung war unzutreffend.

In ca. 40 weiteren Fällen wurden aufgrund eines schweren Fehlers in der Datenverarbeitung Bürger als Kunden der Versicherung angeschrieben.

Die unzutreffend als Kfz-Versicherungsnehmer angeschriebenen Bürgerinnen und Bürger waren allesamt Kunden einer Bank, die zum Zweck der *Kundenaquise* mit der Versicherung kooperiert. Die Bank hatte bei ihren Kunden 1996 ein so genanntes *Mailing* durchgeführt, um bei den Bankkunden für den Abschluss einer Sterbeversicherung der betreffenden Versicherung zu werben. Dabei war eine Weitergabe der Adressdaten der Bankkunden an die Versicherung erfolgt, welche die Werbeschreiben versandte. Bereits die Zulässigkeit der Weitergabe von Kundendaten durch die Bank ist äußerst zweifelhaft. Die Versendung der Werbeschreiben an die Bankkunden führte die Versicherung mit Hilfe ihrer eigenen EDV-gestützten Mitgliederverwaltung durch. Dabei erhielten die übergebenen 20 000 Bankkundenadressen als „Interessenten“ Mitgliedernummern der Versicherung. Diese Nummern wurden einem abgesetzten Nummernkreis entnommen, der bei regulärem Verlauf erst nach Jahren in Anspruch genommen würde. Jedoch übernahm die Versicherung im Folgenden 40 000 Versicherungsverträge, die bislang extern verwaltet wurden, in seine eigene Mitgliederverwaltung. Da die Anzahl der zu verwaltenden Neukunden größer war als die Lücke im Nummernkreis zwischen Altkunden der Versicherung und den als „Interessenten“ aufgenommenen Bankkunden, wurden bereits an diese vergebene Mitgliedernummern doppelt an die übernommenen Kfz-Versicherungsnehmer vergeben. Des weiteren wurde versäumt, die Daten der Bankkunden, die für das bereits zwei Jahre zuvor durchgeführte Mailing verwendet wurden, zu löschen. Daher wurden die Daten der Bankkunden, deren Mitgliedsnummern zweifach vergeben wurden, durch die Daten der neuen Kfz-Versicherungsnehmer ergänzt. Dies führte letztlich dazu, dass Adressaten eines zwei Jahre zurückliegenden Werbeschreibens Versicherungsnachträge für unbekannte Fahrzeuge erhielten.

Diese peinliche Panne wurde nur aufgrund mehrerer Fehler in der Datenverarbeitung durch die Versicherung ermöglicht:

1. Die Adressdaten des vor Jahren abgeschlossenen Bankenmailings waren in dem Datenbestand der Versicherung nicht gelöscht worden, obwohl sie nicht weiter benötigt wurden.
2. Das Mitgliederverwaltungssystem der Versicherung hatte keine Plausibilitätskontrolle. Anderenfalls wäre es rechtzeitig aufgefallen, dass Mitgliedernummern zweifach vergeben wurden.
3. Ein Fehler in der Datenverwaltung ist auch darin zu sehen, dass die Verwaltung von Adressdaten der Bankkunden im Zusammenhang mit dem Werbeschreiben mit der gleichen Datenstruktur und auf dem gleichen Datenbestand wie die eigene Mitgliederdatei der Versicherung erfolgte. Hätte man den Werbekunden eine eigene Datei mit unabhängigen Nummernkreisen gewidmet, wäre eine Überschneidung mit der Mitgliederverwaltung ausgeschlossen gewesen.

4.6.2 Auskunfteien

SCHUFA-Score

Die Schutzgemeinschaft für allgemeine Kreditauskünfte *(SCHUFA)* übermittelt neben der herkömmlichen SCHUFA-Auskunft einen Score, der bei der Beurteilung der Kreditwürdigkeit von Kunden durch Vertragspartner der SCHUFA (z. B. Banken, Versandhandelsunternehmen) helfen soll.

Bei dem *Score-Wert* handelt es sich um einen Punktwert (1 bis 1000) und eine in Prozent ausgedrückte relative Quote, die eine statistische Aussage darüber trifft, mit welcher Wahrscheinlichkeit damit zu rechnen ist, dass bei einer Personengruppe mit bestimmten SCHUFA-Merkmalen in Zukunft Störungen bei der Abwicklung von Kreditverträgen (z. B. Zahlungsunfähigkeit) eintreten werden. Der Score-Wert wird ausschließlich anhand des bereits vorhandenen Datenpools der SCHUFA ermittelt. Er wird an die Vertragspartner der SCHUFA, die an dem Scoring-Verfahren teilnehmen, zusammen mit der üblichen Auskunft übermittelt. Liegt zu einer Person bereits ein so genanntes Negativmerkmal (z. B. eidesstattliche Versicherung) vor, wird kein Score-Wert errechnet.

Die in vielen Wirtschaftsbereichen in Mode gekommenen Scoring-Verfahren sind aus Sicht des Datenschutzes kritisch zu beobachten, weil sie die Gefahr bergen, dass sachwidrige Kriterien (z. B. Nationalität, Qualität einer Wohngegend) allein aufgrund ihrer statistischen Relevanz für die Bonitätsbeurteilung herangezogen werden[167]. Insofern ist es positiv zu bewerten, dass das Scoring-Verfahren der SCHUFA im Sinne einer *Score-Ethik* darauf verzichtet, auf bestimmte Informationen des Datenbestandes (z. B. Geschlecht, Alter, Wohnlage) zurückzugreifen. Auch wenn es statistisch zutreffend sein mag, dass beispielsweise bei Personen, die viele Kredite aufgenommen haben oder häufig ihren Wohnort wechseln, ein höheres Kreditrisiko besteht, so kann dies bei einem Kunden im Einzelfall unzutreffend sein. Daher schreibt die Europäische Datenschutzrichtlinie vor, dass grundsätzlich keine rechtlich erhebliche Entscheidung gegenüber einer Person ergehen darf, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zweck der Bewertung ihrer Kreditwürdigkeit ergeht (Art. 15 Abs. 1).

Die Übermittlung personenbezogener Daten von Vertragspartnern an die SCHUFA erfolgt auf Grundlage der so genannten SCHUFA-Klausel. Diese Klausel wird beispielsweise bei der Eröffnung eines Girokontos durch den Kunden unterzeichnet und lässt die Übermittlung von Informationen „zur Beurteilung der Kreditwürdigkeit“ des Kunden an die SCHUFA zu. Die Einwilligungserklärung ist jedoch nur wirksam, wenn die Betroffenen über den Verwendungszweck der übermittelten Daten im Einzelnen informiert werden. Daher ist eine *Information des Betroffenen* über das Scoring-Verfahren entweder durch Ergänzung der SCHUFA-Klausel oder durch Aushändigung eines gesonderten Merkblattes bei dem Abschluss des Kreditvertrages zwingend erforderlich.

Der Score-Wert ist nicht als solcher in dem Datensatz der SCHUFA gespeichert, sondern wird bei einer Anfrage auf Grundlage der im jeweiligen Zeitpunkt vorliegenden Daten mit Hilfe einer Score-Software ermittelt. Alle Bürgerinnen und Bürger haben einen gesetzlichen Anspruch auf Kenntnis der zu ihrer Person gespeicherten Daten[168]. Sobald der das statistische Verhalten einer bestimmten Personengruppe beschreibende Score-Wert einer einzelnen Person zugeordnet wird, handelt es sich um ein personenbezogenes Datum. Aus der Sicht der Betroffenen ist die jederzeitige Ermittelbarkeit eines personenbezogenen Datums mittels eines technischen Verfahrens der dauerhaften Fixierung einer Information auf dem Datenträger vergleichbar. Für Bürger ist es nicht vermittelbar, dass beispielsweise Banken im Rahmen einer Kreditanfrage bei der SCHUFA deren Score-Wert jederzeit erfragen können, dem Betroffenen dieses Datum jedoch verschlossen bleibt. Aus rechtspolitischer Sicht ist daher zu fordern, dass die SCHUFA eine kurzfristige (z. B. 6-monatige) Speicherung von an Vertragspartner übermittelten Score-Auskünften in einer Zwischendatei vornehmen sollte, um die Betroffenen im Rahmen der *Eigenauskunft* über in der Vergangenheit an Dritte übermittelte Score-Daten informieren zu können.

167 vgl. JB 1997, 4.6.1

168 § 34 Abs. 1 Nr. 1 BDSG

Missbrauch von Auskunfteidaten

In einem Scheidungsverfahren legte der Ehemann zur Verhinderung von Unterhaltsansprüchen seiner Ehefrau die Auskunft einer Wirtschaftsauskunftei vor, wonach diese einer Berufstätigkeit nachgehe, über Ersparnisse verfüge und einen PKW besitze. Jede dieser Informationen war unzutreffend. Insbesondere überraschte aber, dass eine Privatperson Auskünfte von einer Auskunftei erhielt, obwohl die Kunden der Auskunftei ausschließlich Unternehmen sind.

Der Ehemann gelang mit Hilfe seines Vetters, der Inhaber eines Autohauses ist, in den Besitz der Auskunft. Auskunfteien dürfen ihren Kunden nur dann personenbezogene Daten übermitteln, wenn diese ein berechtigtes Interesse an diesen Daten glaubhaft dargelegt haben (§ 29 Abs. 2 Nr. 1a BDSG). Der Autohausinhaber gab gegenüber der Wirtschaftsauskunftei an, er benötige die angeforderten Daten zur Bonitätsüberprüfung, da die Betroffene Kundin seines Autohauses sei und er ihr gegenüber in Vorleistung (z. B. Leasingvertrag) treten wolle.

Damit hat sich der Inhaber des Autohauses nach § 43 Abs. 2 Nr. 1 BDSG strafbar gemacht. Nach dieser Norm wird bestraft, wer die Übermittlung von durch das Bundesdatenschutzgesetz geschützten *personenbezogenen Daten,* die nicht offenkundig sind, *durch unrichtige Angaben erschleicht.*

Auskunfteien sind grundsätzlich nicht verpflichtet, in jedem Einzelfall die Richtigkeit der Angaben ihrer Kunden hinsichtlich des Interesses an der Datenübermittlung zu überprüfen. Eine schlichte Erklärung des Empfängers kann als glaubhafte Darlegung genügen, wenn nach den Gesamtumständen und der Lebenserfahrung eine überwiegende Wahrscheinlichkeit für das Vorliegen der behaupteten Tatsache spricht. Da sowohl der Inhaber des Autohauses als auch die Betroffene den gleichen (nicht sehr häufigen) Namen hatten, hätte die Auskunftei im vorliegenden Fall allerdings vor der Übermittlung eine genauere Überprüfung vornehmen müssen.

Beauskunftung staatsanwaltschaftlicher Ermittlungsverfahren

Eine Wirtschaftsauskunftei speicherte in dem Datensatz des betroffenen Bürgers das Vorliegen „staatsanwaltschaftlicher Ermittlungen wegen Wirtschaftsvergehen". Der Auskunft war nicht zu entnehmen, wie die Auskunftei an diese Information gelangte.

Ein Kreditinformationssystem wird nur dann rechtmäßig betrieben, wenn es so organisiert ist, dass die *Vollständigkeit und Aktualität der gespeicherten Daten* garantiert wird[169]. Die Auskunftei behauptete, durch kurze Wiedervorlagen sei es ihr möglich, die Aktualität des Datenbestandes sicherzustellen. Kurze Wiedervorlagen helfen allerdings nur, wenn die Auskunftei auch die Möglichkeit hat, an zutreffende Daten über den Stand von Ermittlungsverfahren zu gelangen. Die Staatsanwaltschaft darf keine Daten an Auskunfteien herausgeben. Rückfragen können somit in der Regel nur bei der Informationsquelle erfolgen. Häufig dürfte es sich bei dieser um die Presse oder sonstige Medien handeln. Diese Informationsquelle birgt die Gefahr, dass sich die Medien etwa für die Verhaftung oder für die Einleitung eines Strafverfahrens interessieren, die Einstellung eines Verfahrens dagegen keine Schlagzeile und folglich keine Recherche wert ist. Auch bei anderen Informationsquellen (z. B. Informanten) ist zweifelhaft, ob diese in der Lage sind, zuverlässige aktuelle Informationen über ein laufendes Strafverfahren zu geben.

Auch wenn die nach der Rechtsprechung erforderliche Vollständigkeit und Aktualität von Kreditinformationssystemen durch Wiedervorlagen zu gewährleisten sein sollte, ist im Einzelfall zu prüfen, ob ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Speicherung und Übermittlung von Daten über ein laufendes Ermittlungsverfahren besteht (vgl. § 29 Abs. 1 und 2 BDSG). Es ist eine Abwägung der Interessen der Kunden einer Auskunftei, ihr Risiko bei der Vergabe von Geld- bzw. Warenkrediten gering zu halten, mit dem Interesse des Betroffenen, vor den wirtschaftlichen Folgen unzutreffender Beschuldigungen verschont zu bleiben, vorzunehmen. Bei der Interessenabwägung ist § 35 Abs. 2 Satz 2 Nr. 3 BDSG zu beachten. Danach sind personenbezogene Daten zu löschen, wenn es sich um Daten über strafbare Handlungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann. Dieser Norm liegt der im Strafprozessrecht verankerte Rechtsgedanke der *Unschuldsvermutung* zugrunde, wonach an den Verdacht einer Straftat, solange diese nicht erwiesen ist, keine für den Betroffenen negativen Folgen geknüpft werden dürfen. Im Wirtschaftsverkehr wird die Speicherung eines Ermittlungsverfahrens wegen einer vermögensbezogenen Straftat kaum andere Wirkungen haben als die Speicherung der Straftat selbst. Es kann davon ausgegangen werden, dass der Betroffene erhebliche wirtschaftliche Nachteile erleidet. Die Vorgabe, nur beweisbare strafbare Handlungen zu speichern, sollte grundsätzlich nicht dadurch umgangen werden, dass nicht die Straftat selbst, wohl aber das Vorliegen eines Ermittlungsverfahrens gespeichert wird.

Daher kann nur bei Vorliegen sehr strenger Kriterien ausnahmsweise die Rechtmäßigkeit der Speicherung und Übermittlung von Daten über laufende Ermittlungsverfahren angenommen werden:

- Bei dem verfolgten Delikt handelt es sich um eine schwer wiegende Vermögens- bzw. Wirtschaftsstraftat.
- Die Information wurde aus einer öffentlich zugänglichen Quelle (Medien) entnommen.

[169] BGHZ 95, 362, 367

– In der Auskunft wird die Quelle ausdrücklich erwähnt.
– Der Betroffene sollte über die Speicherung des Merkmals „staatsanwaltschaftliches Ermittlungsverfahren“ informiert werden. Hierdurch erhält er Gelegenheit, gegen fehlerhafte Einmeldungen vorzugehen und der Auskunftei das Ende des Ermittlungsverfahrens mitzuteilen.

4.6.3 Verschiedene Unternehmen

Die Regenwasserabgabe und ihre Folgen

Mit dem Ziel einer verursachergerechten Gebührenerhebung planen die Berliner Wasserbetriebe (BWB), in Zukunft die Entgelte für die Ableitung von Schmutz- und Niederschlagswasser getrennt zu erheben. Die Höhe der neu zu berechnenden Regenwasserabgabe wird sich nach der Größe der versiegelten Grundstücksfläche berechnen. Daher benötigen die BWB zur Gebührenberechnung Angaben über die Größe und die Lage des Grundstücks, die Größe der bebauten Fläche und die Art der Flächenversiegelung sowie Angaben zu einer evtl. Eigennutzung von Niederschlagswasser.

Die BWB haben für eine Berechnung des *Niederschlagswasserentgeltes* auf die Unterlagen der Liegenschaftsverwaltungen zurückgegriffen und diese mit aktuellen Luftbildern ergänzt und digitalisiert. Auf den Erfassungsblättern sind die versiegelten Flächen erkennbar. Zur weiteren Überprüfung werden nun die einzelnen Erfassungsblätter nach einem Abgleich mit der *Kundenkartei* an den jeweiligen Verpflichteten gesandt mit der Bitte um Abgleichung und Vervollständigung der Daten.

Eine Übermittlung von Daten der Liegenschaftsverwaltung an die BWB ist bereits jetzt in § 28 Abs. 1 Nr. 2 des Gesetzes über das Vermessungswesen in Berlin (VermG) bereichsspezifisch geregelt. Soweit ein automatisiertes Abrufverfahren durch die BWB geplant sein sollte, wäre die Liegenschaftskataster-Abgabenverordnung, die abschließend die öffentlichen Stellen benennt, die automatisierte Abrufe durchführen dürfen und an die damit eine Datenübermittlung erfolgen kann, durch Aufnahme der BWB zu ergänzen. Durch eine Änderung dieser Rechtsverordnung können die datenschutzrechtlichen Voraussetzungen für eine Übermittlung von Daten aus dem *Liegenschaftskataster* an die BWB geschaffen werden. Außerdem sind in § 4 der Verordnung über die Verarbeitung personenbezogener Daten bei den Berliner Stadtreinigungsbetrieben, den Berliner Verkehrsbetrieben und den Berliner Wasserbetrieben (BerlBetrDatVO) die personenbezogenen Grundstücksdaten mit aufzunehmen, die zur Berechnung der Regenwasserabgabe erforderlich sind. Eine entsprechende Änderung der Rechtsverordnung ist zu erwarten.

Vorgetäuschte Meinungsumfragen

Wir erhielten mehrere Beschwerden gegen ein im Immobiliengeschäft tätiges Unternehmen, das Mitarbeiter beschäftigte, deren Aufgabe es war, in wohlhabenden Wohngegenden lebende Bürgerinnen und Bürger anzurufen und unter dem Vorwand, sie seien für ein „Institut für Informationsaustausch Berlin/Brandenburg“ tätig, diese zu ihren Befürchtungen vor finanziellen Einbußen aufgrund der Euro-Einführung sowie deren Einkünften und der familiären Lebenssituation zu befragen. Die Betroffenen machten zahlreiche Angaben in der Annahme, bei der Befragung handele es sich um eine anonymisierte Meinungsumfrage. Erst bei einem zweiten Anruf, bei dem das Unternehmen unter seinem wirklichen Namen auftrat und Beratungsleistungen zu Vermögensfragen anbot, offenbarte sich den Betroffenen, dass die Daten zusammen mit ihrem Namen und Telefonnummer zum Zweck der Kundenakquise aufgezeichnet worden waren.

Nach § 28 Abs. 1 Satz 2 BDSG müssen personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Die Angabe, für ein „Institut für Informationsaustausch“ tätig zu sein, sowie die Fragen zur Euro-Angst dienten dazu, die Angerufenen über den Gesprächspartner und den Zweck der Befragung zu täuschen, indem der Eindruck erweckt wurde, mit einem Markt- und Meinungsforschungsinstitut zu sprechen. Diese Datenerhebung verstößt gegen Treu und Glauben und ist damit rechtswidrig.

Bei einer von uns durchgeführten Prüfung in den Betriebsräumen des Unternehmens vergewisserten wir uns davon, dass die bei den Beschwerdeführern erhobenen Daten nicht länger gespeichert wurden, nachdem es zu keinem Beratungsgespräch gekommen war. Der Geschäftsführer des Unternehmens versicherte uns, die aus datenschutzrechtlicher Sicht unzulässige Akquisepraxis eingestellt zu haben. Uns wurden entsprechende schriftliche Anweisungen an die Mitarbeiter des Unternehmens vorgelegt.

Datenspuren bei Bahnreservierungen

Mehrere Kunden der Deutschen Bahn AG beschwerten sich über Datenspuren bei telefonischen Reservierungen von Fahrausweisen. Sie mussten Name, Anschrift, Telefonnummer, in einem Fall den Beruf, die Bankverbindung und die BahnCardnummer angeben sowie nähere Angaben bezüglich der gebuchten Reise machen, die dann unter einer „Kundennummer“ gespeichert wurden.

Seit dem 1. Juni 1997 werden telefonische Bestellungen von Reisedokumenten mit dem Verfahren *„Bahnreise-Bestell-Service“ (BABS)* elektronisch aufgenommen und abgewickelt. Bei der Aufnahme der Bestellung werden die für ihre Ausführung notwendigen Kundendaten erfasst. Bei Abholbestellungen sind der Familienname sowie die Post-

leitzahl und der Ortsname der Anschrift des Kunden erforderlich, damit bei der Abholung der Unterlagen eine Identifizierung stattfinden kann, wobei die bei der Bestellung gleichfalls vergebene Kundennummer die Zuordnung erleichtert. Die genaue Anschrift wird nur bei Versandbestellungen erhoben. Die Speicherung weiter gehender Daten ist für die Erfüllung des (sich anbahnenden) Vertrages nicht erforderlich (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).

Die bei Bestellannahme erfassten Kundendaten werden bis zur Erledigung der Bestellung (Aushändigung der Dokumente gegen Bezahlung bzw. Tag der Reise) sowie für daran sich anschließende sechs Monate gespeichert, um mögliche vom Kunden vorgetragene Unregelmäßigkeiten bearbeiten zu können. Nach Ablauf dieser Frist werden die Daten gelöscht, es sei denn, in diesem Zeitraum erfolgt eine weitere telefonische Bestellung des Kunden. In diesem Fall kann auf die bereits vorhandene Kundennummer zurückgegriffen werden, so dass die Kundendaten bei der nächsten Bestellung nicht nochmals eingegeben werden müssen. Gegen die 6-monatige „Nachspeicherdauer“ bestehen keine Bedenken, weil sich während dieses Zeitraums Nachfragen der Betroffenen bzw. rechtliche Auseinandersetzungen ergeben können (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG).

Kunden, die eine derartige Datenspeicherung nicht wünschen, haben nur die Möglichkeit des Direktbezugs der Reiseunterlagen bei einer Fahrkartenausgabestelle bzw. einem Reisebüro.

Busreise mit Hindernissen

Die Kundin eines Busreiseunternehmens beschwerte sich darüber, dass sie bei Fahrtantritt einer vorab gebuchten Reise als Sicherheit dafür, dass sie den Reisepreis gezahlt hat, neben ihren Personalien auch ihre Personalausweis- bzw. Passnummer in eine „Zahlungsbestätigung“ eintragen sollte. Die Kundin hat nur deshalb ihre Ausweisnummer eingetragen, weil sie anderenfalls aus dem Bus hätte aussteigen müssen.

Das Reiseunternehmen verlangte diese Angaben von Teilnehmern, die ihre Reise so kurzfristig buchen und bezahlen, dass eine Kontrolle des Zahlungseingangs vor Beendigung der Reise nicht möglich ist. Die Angaben sollten dem Zweck dienen , den Reiseteilnehmer im Fall einer Falschangabe über die angeblich geleistete Zahlung zu identifizieren und gerichtlich in Anspruch nehmen zu können.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Speichern personenbezogener Daten zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses. Wird der Reisepreis von dem Teilnehmer nicht entrichtet, so bedarf es allein des Namens sowie der Anschrift des Kunden, um ihn zivilrechtlich in Anspruch nehmen zu können. Die Personalausweis- oder Passnummer wird zu diesem Zweck nicht benötigt. Sie kann darüber hinaus nicht dazu dienen, im Fall einer Nichtzahlung den Kunden identifizieren zu können, da das Pass- und Ausweisregister führende Landeseinwohneramt zu einer Übermittlung von Angaben aufgrund der Seriennummer nicht befugt ist. Nichts anderes ergibt sich aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Das berechtigte Interesse des Reiseunternehmens (an der zivilgerichtlichen Verfolgung) kann allein dadurch gewahrt werden, dass der Name und die gegenwärtige Anschrift des Betroffenen (nach Vergleich mit den im vorgelegten Ausweis oder Pass enthaltenen Angaben) für den erforderlichen Zeitraum gespeichert werden (vgl. § 35 Abs. 2 Satz 2 Nr. 3 BDSG).

Das Reiseunternehmen wird künftig die Pass- bzw. Personalausweisnummer der Reiseteilnehmer nicht mehr in die so genannte „Zahlungsbestätigung“ aufnehmen und ihre Formulare ändern.

Verletzung des Bankgeheimnisses durch Detektei

Ein Petent stand in dem Verdacht, einen Betrug zulasten seiner Reiseversicherung begangen zu haben. In zwei Fällen hatte er angegeben, auf einer Urlaubsreise bestohlen worden zu sein. Da Ungereimtheiten vorhanden waren, wollte die Versicherung den Schaden nicht begleichen. Der Petent trug u. a. vor, sein Konto bei der Landesbank Berlin weise ein Guthaben von über 700 000 DM auf und er habe es somit nicht nötig zu betrügen. Er legte einen entsprechenden Buchungsbeleg der Landesbank Berlin vor.

Obwohl der Vortrag des Petenten, er verfüge über ein entsprechendes Guthaben bei der Landesbank Berlin, kein sachliches Argument dafür darstellt, einen *Betrugsverdacht* auszuräumen, sah sich die *Reiseversicherung* veranlasst, durch eine von ihr beauftragte *Detektei* überprüfen zu lassen, ob der Petent tatsächlich über ein entsprechendes Guthaben verfügt. Der daraufhin von der Detektei erstellte Ermittlungsbericht lautete folgendermaßen:

„Unter Einschaltung von Gewährsleuten wurden Ermittlungen bezüglich des vom Versicherungsnehmer vorgelegten Bankauszuges vorgenommen. Nach Einsicht in die Kontoführungsunterlagen (EDV) erhielten wir ferner die Bestätigung, dass am 19. 9. 1997 diesem Konto ein Betrag in Höhe von 700 000 DM zunächst gutgeschrieben, jedoch zur gleichen Zeit wieder storniert bzw. abgebucht wurde (. . .). In diesem Zusammenhang konnte ferner in Erfahrung gebracht werden, dass auf dem Konto des Versicherungsnehmers in zurückliegender Zeit keine fünf- oder sechsstelligen Beträge vorhanden waren, im Gegenteil, des Öfteren kam es sogar zu Minusbeträgen.“

Indem die Detektei sich Einsicht in die *Kontodaten* des Petenten verschafft hat, hat sie sich nach § 43 Abs. 1 Ziff. 3 BDSG strafbar gemacht. Nach dieser Vorschrift handelt strafbar, wer unbefugt von dem Bundesdatenschutzgesetz geschützte personenbezogene Daten, die nicht

offenkundig sind, abruft oder sich oder einem anderen aus Dateien verschafft. Nachdem der Petent einen Strafantrag gegen die Detektei gestellt hat, läuft nun ein Ermittlungsverfahren gegen diese.

Die *Landesbank Berlin* konnte nicht aufklären, wie der Zugriff auf die geschützten Kontodaten erfolgen konnte. Möglicherweise handelte es sich jedoch bei den in dem Detekteibericht genannten „Gewährsleuten" um Mitarbeiter der Bank. In der Einsichtsgewährung in die Kontounterlagen durch Bankmitarbeiter läge sowohl eine Verletzung von Vorschriften des Bundesdatenschutzgesetzes als auch eine Verletzung des vertraglich gegenüber dem Bankkunden bestehenden *Bankgeheimnisses.*

In der von uns durchgeführten Überprüfung stellten wir mit Erstaunen fest, dass die Reiseversicherung sich offenbar nicht bewusst war, dass der an die Detektei erteilte Ermittlungsauftrag datenschutzrechtlich problematisch war. Sie vertrat uns gegenüber die Auffassung, dass der Petent, indem er den Buchungsbeleg über 700 000 DM freiwillig vorgelegt habe, sich implizit mit einer Überprüfung der Richtigkeit dieser Angaben einverstanden erklärt habe. Diese Auffassung ist schon deshalb nicht haltbar, weil eine Einwilligung im Sinne des Bundesdatenschutzgesetzes voraussetzt, dass diese ausdrücklich und schriftlich erteilt wird (§ 4 Abs. 2 BDSG).

Elektronische Mehrfachkarten der Berliner Bäderbetriebe

Die Berliner Bäderbetriebe erweiterten im Jahr 1998 das EDV-unterstützte Eintrittskartensystem. Zu Beschwerden führte die im Bad am Spreewaldplatz eingeführte Mehrfachkarte. Beim Kauf dieser Karte wurden Name und Vorname des Kunden abgefragt und in den Kassencomputer eingegeben. Die zum mehrfachen Eintritt berechtigende Barcodekarte enthält einen Aufdruck des Kundennamens. Beim Passieren des elektronischen Drehkreuzes werden auf diese das Ende der zulässigen Badezeit und die verbleibenden Eintrittsberechtigungen angezeigt.

Bei dem Verkauf von *Sammelkarten* erfolgt die Angabe von Name und Vorname des Kunden auf freiwilliger Basis. Eine Identitätsprüfung, wie sie beispielsweise für ermäßigte Eintrittskarten oder nicht übertragbare Halbjahres- oder Jahreskarten erforderlich ist, erfolgt nicht. Die Speicherung des Namens im Kassencomputer erfolgt zu dem Zweck, bei Verlust oder Beschädigung der Dauerkarte dem Kunden einen Ersatz zu ermöglichen.

Nach § 6 Abs. 1 BlnDSG ist eine Speicherung personenbezogener Daten u. a. dann zulässig, wenn der Betroffene eingewilligt hat. Die Einwilligung ist jedoch nur dann wirksam, wenn sie freiwillig erfolgt. Daher müssten die Kunden vor Kauf der Sammelkarte beispielsweise durch einen *Aushang im Kassenbereich* darauf hingewiesen werden, dass ein Kauf der Sammelkarte auch ohne Namensangabe bzw. Angabe eines

Pseudonyms erfolgen kann. Die Kunden sollten darauf aufmerksam gemacht werden, dass bei Verlust einer Sammelkarte eine Erstattung des entsprechenden Restguthabens nur dann erfolgen kann, wenn der betreffende Kunde durch eine entsprechende Identifizierung nachweisen kann, berechtigter Inhaber der verlorenen Karte zu sein. Es ist aus datenschutzrechtlicher Sicht unproblematisch, dass der Kunde, wenn er sein Wahlrecht dahin ausübt, beim Kauf der Karte keinen Namen bzw. ein Pseudonym anzugeben, das Risiko des Verlustes der Karte selbst trägt.

4.7 Internationaler und Europäischer Datenschutz

Am 24. Oktober 1998 ist die von der europäischen Richtlinie zum Datenschutz *(EU-Richtlinie)* vorgegebene Frist zur *Umsetzung* ihrer Regelungen in nationales Recht abgelaufen[170]. Die Mitgliedstaaten hatten drei Jahre Zeit, um ihre Rechtsvorschriften den Anforderungen der EU-Richtlinie anzupassen[171]. Als sich Mitte 1998 abzeichnete, dass der bundesdeutsche Gesetzgeber in der ablaufenden Legislaturperiode eine Änderung des Bundesdatenschutzgesetzes nicht mehr auf den Weg bringen würde, haben wir die seit Jahren unter dem Vorsitz Berlins geführte Arbeitsgruppe „Internationaler Datenverkehr" des Düsseldorfer Kreises[172] einberufen, um die mit der fehlenden Umsetzung der Richtlinie zusammenhängenden Fragen einer einheitlichen Klärung zuführen zu können. Im Vordergrund stand dabei die Problematik, wie sich die Aufsichtsbehörden zu verhalten haben, wenn ein Unternehmen mit Sitz im Bundesgebiet personenbezogene Daten ins Ausland übermitteln will. Für den Export in außereuropäische Staaten (Drittländer) verpflichtet die Richtlinie die Mitgliedstaaten der Union, die *grenzüberschreitende Datenübermittlung* nur in solche Länder zuzulassen, in denen ein angemessenes Datenschutzniveau gewährleistet ist (Art. 25 EU-Richtlinie). Ausnahmsweise kann eine Datenübermittlung in ein Drittland, das kein angemessenes Schutzniveau gewährleistet, unter den in Art. 26 EU-Richtlinie genannten Fällen vorgenommen werden.

Die Arbeitsgruppe kam zunächst darin überein, dass die von ihr im Jahre 1996 erarbeiteten Leitlinien zur Übermittlung personenbezogener Daten in Länder ohne angemessenes Datenschutzniveau nicht mehr angewendet werden sollen[173], sondern abgelöst sind durch die (wenngleich teilweise übereinstimmenden) Grundsätze, die die Arbeitsgruppe nach Art. 29 EU-Richtlinie in einer Arbeitsunterlage WP 12 vom 24. Juli 1998 dargelegt hat[174]. Die in dem Papier genannten inhaltlichen und verfahrensrechtlichen Grundsätze (z. B. die Beschränkung der Zweckbestimmung, Transparenz gegenüber dem Betroffenen, Mecha-

170 vgl. 1.1
171 JB 1995, 1.2; JB 1997, 1.1
172 vgl. 6.4
173 vgl. JB 1996, 1.1, Anlage 3
174 Anlagenband „Dokumente zum Datenschutz 1998", Teil C

nismen für die Durchsetzung von Betroffenenrechten) sind als Minimalanforderungen zu beachten zur Bestimmung der Angemessenheit des Schutzniveaus bei Rechtsvorschriften, selbstregulierenden Maßnahmen von Unternehmen und bei Verträgen. Als Folge der nicht rechtzeitigen Umsetzung der Richtlinie geht die Arbeitsgruppe davon aus, dass die Richtlinie – entsprechend der zu derartiger Problematik ergangenen Rechtsprechung des Europäischen Gerichtshofs – keine horizontale Direktwirkung entfaltet (private Stellen gegeneinander also keine unmittelbaren Ansprüche aus der Richtlinie herleiten können), sondern lediglich eine vertikale Wirkung im Verhältnis Bürger – Staat[175].

Bei der Beurteilung der Zulässigkeit von Datenübermittlungen in Drittländer sind nach wie vor die §§ 28, 29 BDSG anwendbar. In ihre Generalklauseln, insbesondere bei der Beurteilung der „schutzwürdigen Interessen" des Betroffenen, müssen die Grundsätze der EU-Richtlinie (und die Mindestkriterien des WP 12) einfließen. Der Betroffene kann also auf diesem Wege seine (aufgrund der Richtlinie erweiterten) Rechte gegenüber der Daten verarbeitenden Stelle geltend machen. Erfolgt die Datenverarbeitung im Rahmen des für den Vertragszweck Erforderlichen, so fließen die Grundsätze bei der Vertragsauslegung z. B. über den Grundsatz von Treu und Glauben ein (vgl. § 28 Abs. 1 Satz 2 BDSG).

Bei der Anwendung der Grundsätze der Richtlinie ist zunächst zu beachten, dass die EU-Mitgliedstaaten, auch wenn sie – wie die Bundesrepublik selbst – die Richtlinie noch nicht umgesetzt haben, nicht wie Drittländer zu behandeln sind und deshalb die Angemessenheit des Schutzniveaus bezüglich des empfangenden EU-Staates nicht geprüft werden muss. Bei einem Export in außereuropäische Staaten (Drittländer) ist die Angemessenheit des Schutzniveaus in diesem Drittstaat anhand der Grundsätze der Richtlinie und der auf dieser Grundlage entwickelten Mindestkriterien des Arbeitspapiers WP 12 zu prüfen. Zumeist dürfte die Datenübermittlung nach Art. 26 Abs. 1 a) (Einwilligung des Betroffenen) oder b) EU-Richtlinie (Datenübermittlung für die Erfüllung eines Vertrages mit dem Betroffenen erforderlich) erfolgen. Nur wenn die Tatbestände des Art. 26 Abs. 1 EU-Richtlinie nicht vorliegen, müssen nach Abs. 2 ausreichende Garantien zum Schutz der Rechte Betroffener (z. B. im Rahmen einer vertraglichen Vereinbarung) verlangt werden. Umgekehrt müssen bei Vorliegen einer vertraglichen Vereinbarung nach Art. 26 Abs. 2 nicht noch zusätzliche Voraussetzungen nach Abs. 1 erfüllt sein, es sei denn, es soll von einer im Vertrag nach Art. 26 Abs. 2 enthaltenen Regelung zu Ungunsten des Betroffenen abgewichen werden. In diesem Fall ist die Einwilligung des Betroffenen nach Art. 26 Abs. 1 a) erforderlich. Dies schließt allerdings nicht aus, dass der Datenexporteur auch im Rahmen von Vertragsverhältnissen oder beim Vorliegen von Einwilligungen verpflichtet ist, beim ausländischen Vertragspartner auf hinreichende Datenschutzvorkehrungen hinzuwirken (Art. 17 EU-Richtlinie).

[175] vgl. 1.1

Hinsichtlich der verfahrensmäßigen Vorgehensweise der Unternehmen selbst sowie der Aufsichtsbehörden war die Arbeitsgruppe der Ansicht, dass die Vorschriften über das formelle Genehmigungsverfahren nach Art. 26 Abs. 2 der Richtlinie der näheren Ausgestaltung durch den nationalen Gesetzgeber bedürfen und deshalb bis dahin keine unmittelbare Wirkung für betroffene Unternehmen entfalten. Auch eine Unterrichtungspflicht gegenüber der Europäischen Kommission nach Art. 26 Abs. 3 wird nicht angenommen. Beabsichtigt ist jedoch, die Kommission in Anlehnung an diese Bestimmung über die positive Bewertung der zuständigen Aufsichtsbehörde zu informieren.

Um eine bundeseinheitliche Verfahrensweise der Aufsichtsbehörden bei der Beurteilung von Fällen des grenzüberschreitenden Datenverkehrs zu gewährleisten, hat die Arbeitsgruppe ein Verfahren zur gegenseitigen Information der Aufsichtsbehörden entwickelt, die die jeweils eingegangenen Prüffälle von grundsätzlicher Bedeutung im Zusammenhang mit den Art. 25, 26 der EU-Richtlinie umfasst. Die Informationen sollen aus den zugrunde liegenden Unterlagen und einem entsprechenden Votum der Aufsichtsbehörde bestehen, die die Weiterleitung an die Oberste Aufsichtsbehörde unternimmt. Von dort sind die Informationen an eine koordinierende Stelle (Clearingstelle) weiterzugeben, damit sie die jeweils anderen Obersten Aufsichtsbehörden in Kenntnis setzen kann. Die Funktion dieser „Clearingstelle" haben wir als Vorsitzende der Arbeitsgruppe „Internationaler Datenverkehr" übernommen. Die zuständige Aufsichtsbehörde entscheidet gemäß ihrem Votum, wenn die Obersten Aufsichtsbehörden keine Einwände erhoben haben. Andernfalls wird der Sachverhalt in der Arbeitsgruppe „Internationaler Datenverkehr" – gegebenenfalls im schriftlichen Verfahren – erörtert. Die zuständige Aufsichtsbehörde entscheidet sodann unter Berücksichtigung der Erörterungen der Arbeitsgruppe.

4.8 Organisation und Technik

4.8.1 Technische und organisatorische Datenschutzfragen beim Standardsoftware-Produkt SAP R/3

Eines der erfolgreichsten Softwareprodukte der Welt ist die integrierte, branchenunabhängige Standardsoftware R/3 des deutschen Softwarehauses SAP. Sie kann alle betriebswirtschaftlichen Anwendungsgebiete (z. B. Rechnungswesen, Logistik oder Personalwirtschaft) abdecken.

Allein in der öffentlichen Verwaltung des Landes ist das Produkt in vielfacher Weise im Einsatz: Als Version R/3 ISH wird es in vielen großen Krankenhäusern und Universitätskliniken für die Personal- und

Patientenverwaltung und -abrechnung eingesetzt. Es bildet die Grundlage für die aktuelle Version III der Krankenhausrechnungswesens KRW, welches in den meisten Krankenhäusern bereits im Einsatz ist. Als Version R/3 HR (Human Resources) bildet es die Grundlage für das in Einführung begriffene Integrierte Personalverfahren (IPV) des Landes Berlin. Insbesondere in den öffentlich-rechtlich strukturierten Betrieben des Landes finden sich diverse weitere Anwendungen dieses Produktes. Auch in der Privatwirtschaft des Landes hat das Produkt SAP R/3 in seinen verschiedenen Anwendungsversionen weite Verbreitung gefunden.

Was für Berlin gilt, gilt bundesweit, vermutlich sogar weltweit. Das Produkt SAP R/3 ist die Basis für den Aufstieg der Firma SAP zu einem der erfolgreichsten multinational einflussreichen Unternehmen Deutschlands. Es gibt also für die Informatiker bei den Datenschutzbeauftragten des Bundes und der Länder Gründe genug, sich mit dem außerordentlich komplexen System zu befassen.

Die Software ist *modular aufgebaut.* Daten, die in einem Modul (z. B. Rechnungswesen) erfasst werden, stehen sofort den anderen Modulen (z. B. Logistik) zur Verfügung. Daten müssen somit nur einmal eingegeben werden und die Zahl der Schnittstellen lässt sich auf ein Minimum reduzieren.

Das Prinzip von R/3 beruht darauf, dass mit ihm ein System von Tabellen einer Datenbank verwaltet wird, die in komplexer Weise miteinander in Beziehung stehen. Diese Datenbank kann eine fast beliebige Standardsoftware sein, wie z. B. Adabas-D, Informix oder Oracle, die lediglich die Datenbankabfragesprache SQL (Standard QUERY Language) unterstützen muss. Als Serverbetriebssystem können verschiedene Plattformen (z. B. Unix-Derivate oder Windows NT) herangezogen werden, sofern sie von SAP dafür zertifiziert worden sind.

Diese Plattformunabhängigkeit und die Flexibilität, mit der R/3-Systeme an Betriebs- bzw. Behördenstrukturen durch sog. *„Customizing"* angepasst werden können, macht den Erfolg des Produktes aus. In der breiten Öffentlichkeit ist das Produkt wesentlich weniger populär als die Produkte des Konkurrenten Microsoft, weil es dem Heimanwender nur wenig Nutzen bringt und Ressourcen beansprucht, die die Kapazitäten der üblichen Rechner in privaten Haushalten und kleinen Wirtschaftsbetrieben weit überfordern.

Für eine datenschutzrechtliche Betrachtung von R/3 steht die Ausgestaltung des Berechtigungskonzepts im Vordergrund.

Das *Berechtigungskonzept* im SAP-System ist objektorientiert aufgebaut. Es definiert z. B. als Transaktionen bezeichnete ausführbare Anwendungsprogramme oder einzelne Tabellenfelder als Berechtigungsobjekte und ordnet ihnen Berechtigungen zu (z. B. zur Ausführung eines Programms oder zum lesenden, ändernden oder löschenden

Zugriff auf die Felder). Man kann die Berechtigungsobjekte als Schloss für das System bezeichnen und die Berechtigungen als die Schlüssel ansehen.

Berechtigungsobjekte werden in der R/3-eigenen Programmiersprache ABAP/4 geschrieben. Sie können daher im Zuge der Systemadministration weder ergänzt oder verändert werden.

Zum Öffnen des „Schlosses" *Berechtigungsobjekt* werden die „Schlüssel", nämlich die Berechtigungen, benötigt. Die Differenzierungsmöglichkeiten durch Berechtigungen hängen von der Art des jeweiligen Berechtigungsobjektes ab. So ist z. B. eine Berechtigung zur Ausführung bei einem nicht ausführbaren Objekt, wie z. B. einem Tabellenfeld, sinnlos. Eine solche Berechtigung macht vielmehr nur bei ausführbaren Objekten Sinn, also bei Programmen, bei R/3 Transaktionen genannt. Welche Berechtigungen für ein Berechtigungsobjekt vergeben werden, wird von einem sog. Berechtigungsadministrator festgelegt. Diese Rolle entspricht also der des Schlüsselverwalters.

Den Nutzern werden in Abhängigkeit von ihren am System durchzuführenden Aufgaben Berechtigungen zugewiesen. Zusammengehörende Berechtigungen in Anwendungen können zu „Profilen" zusammengeführt werden. Zur Erhöhung der Übersichtlichkeit können die Profile noch zu „Sammelprofilen" zusammengefasst werden. Die Zugriffsberechtigungen eines Benutzers ergeben sich also aus den ihm zugeordneten Sammelprofilen, Profilen und einzelnen Berechtigungen. Diese persönlich zugeordneten Berechtigungen werden in einen Benutzerstammsatz eingetragen, der alle für das System notwendigen benutzerbezogenen Daten enthält.

Änderungen in Berechtigungen oder Profilen/Sammelprofilen werden erst nach einer neuen Anmeldung des Benutzers wirksam. Änderungen in Berechtigungsobjekten sind sofort wirksam.

Zur Umsetzung des Berechtigungskonzepts bietet das R/3-System die Möglichkeit der *Funktionentrennung innerhalb der Systemadministration.* Im Idealfall wird zwischen vier Funktionen unterschieden:

- Der/die Anwendungsentwickler/in legt Felder und Objekte an und entwickelt so die Berechtigungsobjekte.
- Der/die Berechtigungsadministrator/in pflegt Berechtigungen bzw. Profile und Sammelprofile.
- Der/die Aktivierungsadministrator/in aktiviert Berechtigungen bzw. Profile und Sammelprofile, kann aber ggf. Änderungen vornehmen, die protokolliert werden. Nur aktivierte Berechtigungen bzw. Profile und Sammelprofile können Nutzern zugeordnet werden.
- Der/die Benutzeradministrator/in ordnet Berechtigungen bzw. Profile und Sammelprofile Benutzern zu und pflegt die Benutzerstammsätze.

Das R/3-Berechtigungskonzept erscheint geeignet, die datenschutzrechtliche Idealvorstellung zu realisieren, dass jeder Benutzer exakt die Berechtigungen bekommt, die er für seine Aufgaben benötigt. Allerdings ist es gerade die außergewöhnliche Komplexität des Konzepts, die seine Schwachstellen ausmacht und die in der Fachöffentlichkeit zur Diskussion über die informationstechnische Sicherheit der verbreiteten Standardsoftware geführt hat.

Wir wollen an dieser Stelle exemplarisch einige Risiken ansprechen, die bei der Verwendung von SAP R/3 bekannt geworden sind.

Der Hamburgische Datenschutzbeauftragte hat bereits früher[176] auf das Hauptproblem des Berechtigungskonzepts hingewiesen. Der hohe Grad an Komplexität führt zu einer *Intransparenz,* die die Revision eines R/3-Systems nicht nur für außenstehende Prüfer, wie z. B. die Datenschutzbehörden, schwierig macht. Selbst mit dem System vertraute Personen wie etwa die o. g. Administratoren können Sicherheitslücken leicht übersehen oder gar unbewusst verursachen.

Die Ausarbeitung eines guten Berechtigungskonzepts muss bereits in der Projektierungsphase vorbereitet werden, denn wenn seine Erstellung erst mit der Installation des Systems beginnt, dann sind Fehler fast unvermeidlich. Das folgende Beispiel macht dies plausibel:

Die Standardversion von SAP R/3 (Release 4.x) beinhaltet bereits bei Auslieferung ca. 700 Berechtigungsobjekte. Der Speicherraum für Berechtigungen im Benutzerstammsatz eines einzelnen Benutzers soll mindestens Raum für 1300 Berechtigungseinträge bieten. Da ist es kein Wunder, wenn es Fälle gibt, in denen überforderte Administratoren zur Gewährleistung eines reibungslosen Produktivbetriebs einfachen Benutzern zeitweilig eine *Generalzugriffsberechtigung* auf das gesamte System (SAP_ALL) zugewiesen haben. Dies ist zwar ein Extremfall, aber es besteht grundsätzlich die Gefahr, dass Nutzern mehr als die notwendigen Rechte zugewiesen werden.

Wenn zur Lösung eines bestimmten Problems eine spezielle Berechtigung vergeben wird, ist es standardmäßig nicht möglich auszuschließen, dass unbeabsichtigt Zugriffsrechte in anderen Anwendungen eröffnet werden. Eine entsprechende Prüfung findet durch das System nicht statt.

Es gibt Transaktionen, Tabellenfelder oder Berichte (Reports), die im Berechtigungskonzept nicht als Berechtigungsobjekte definiert sind, damit also kein Schloss besitzen. Ein Schutz muss dann auf Teilstrukturen (Unterprogramme, Teilfelder etc.) wirken, wenn diese ihrerseits Berechtigungsobjekte sind. Anschaulich vergleichbar ist dies mit dem Verschluss von Schränken in einem Raum, weil der Raum selbst nicht verschlossen werden kann.

[176] 14. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, 1995

Ein Beispiel für eine *Transaktion, für die keine Berechtigungsprüfung* durchgeführt wird und die daher von jedem Benutzer ausgeführt werden kann, ist die Transaktion DI02, mit der man sich Dateien und Daten im System ansehen kann, wenn Sicherheitseinstellungen fehlen. Über sie können alternative Wege zu sensiblen Daten eröffnet werden, obwohl die eigentliche Zugriffstransaktion ein Berechtigungsobjekt ist und daher Schutz bietet. Zwar mögen diese Umwege nur wenigen bekannt sein, aber es ist kein Schutzmechanismus, auf die Unkenntnis der Nutzer zu bauen. Anhand dieses Beispieles lässt sich erkennen, dass der Systemadministrator wegen des hohen Komplexitätsgrades von R/3 sehr sorgfältig arbeiten muss.

Für die oben geschilderten Sicherheitsprobleme werden Werkzeuge mit verschiedenen Lösungsansätzen von anderen Herstellern angeboten. Es ist jedoch bei Experten umstritten, ob Aufwand und Nutzen bei diesen Produkten in einem vernünftigen Verhältnis stehen.

Ein großes Sicherheitsproblem bilden die *SAP-Standardprofile,* die zusammen mit dem System ausgeliefert werden, wenn sie unkontrolliert in das Produktivsystem übernommen werden. Im Allgemeinen geben sie den Benutzern zu viele Rechte. Sie sollten daher nur als Vorlage für selbst zu definierende Profile dienen. Dann erst erschließen sich die Vorteile, weil man die Zugriffsprofile auf den tatsächlichen Bedarf anpassen kann. Außerdem bleibt man unabhängig von den Veränderungen der Standardprofile, die bei Releasewechseln erfolgen, denn die eigenen Profile bleiben dann unverändert.

Bei jedem *Releasewechsel* ist zu beachten, dass nur eine bearbeitete Version des Standardprofils SAP-NEW im System verbleibt. Jeder Benutzerstammsatz beinhaltet dieses Profil. In der unbearbeiteten Version enthält es alle Berechtigungen für neu hinzugekommene Berechtigungsobjekte. Bei einem Releasewechsel bestünde dann die Gefahr, dass Nutzer zu viele oder sogar Generalzugriffsberechtigungen erhalten.

Ein weiteres Risiko steckt im *Kernel* des R/3-Systems. Dort wurde der Pseudonutzer SAP* für die Erstinstallation fest implementiert, der uneingeschränkte Zugriffsberechtigungen auf das System hat und nicht gelöscht werden kann. Eine Sicherung gegen unbefugte Nutzung dieses privilegierten Zugangs ist nur möglich, wenn dazu ein Benutzerstammsatz angelegt wird, in dem das Kennwort verändert und alle Berechtigungen gelöscht wurden.

R/3 bietet die Möglichkeit, den Nutzer zu einem *periodischen Kennwortwechsel* zu zwingen. Dabei können vorher definierte Trivialkennwörter verboten werden. Initialkennwörter, die nur für das erstmalige Anmelden am System vergeben werden, unterliegen diesen Beschränkungen nicht. Dies wäre unkritisch, wenn es im R/3-System nicht möglich wäre, alle Kennungen zu ermitteln, die sich vorher noch nie am

System angemeldet haben. Da das Initialkennwort üblicherweise den meisten Benutzern bekannt ist, weil immer das gleiche Verwendung findet, entsteht ein nicht unerhebliches Gefahrenpotential. Hier sollte nach den „Empfehlungen des Berliner Datenschutzbeauftragten für die Vergabe von Passwörtern“[177] vorgegangen werden.

Ein oft unterschätztes Problem bei der Einrichtung von Benutzerstammsätzen ist die *Vergabe von Druckrechten.* Im R/3-Standard dürfen Nutzer mit einem beliebigen Ausgabegerät drucken. Wenn dieses Recht nicht eingeschränkt wird, könnten u. U. vertrauliche Daten auf frei zugänglichen Druckern ausgegeben werden.

Das beste Berechtigungskonzept ist wenig wert, wenn es umgangen werden kann. Um eine möglichst große Vielzahl von Plattformen bedienen zu können, setzt SAP auf Standarddatenbank-Softwareprodukten auf. Werden dafür keine besonderen Sicherheitsmaßnahmen getroffen, kann auf die Daten unter Umgehung des Systems R/3 zugegriffen werden. Da R/3 seine Daten unverschlüsselt ablegt, kann auf eine solche Schutzfunktion nicht gebaut werden. Für den Datenbankserver sollten *nur zwei lokale Kennungen,* eine für die Systemverwaltung und eine für das R/3-System, existieren. Individuelle Kennungen sind zu vermeiden.

Mit der wachsenden Verbreitung der SAP-Software hat der Hersteller dem Datenschutz eine höhere Priorität zugewiesen. So wurde in diesem Jahr erstmalig ein *Datenschutzleitfaden* herausgegeben, der z. T. ins Detail gehende Hinweise für eine datenschutzgerechte Ausgestaltung gibt[178].

Um den erwähnten Risiken der Unüberschaubarkeit des Berechtigungskonzepts entgegenzutreten, wurde seit dem Release 3.1x ein *Profilgenerator* zur Erleichterung der Administration eingeführt, der fortlaufend weiterentwickelt wird. Bei den Anwendern stößt dieser aufgrund der noch hohen Fehleranfälligkeit auf ein geteiltes Echo. Es ist zu hoffen, dass SAP in späteren Versionen mit diesem Werkzeug eine ausreichende Transparenz erreicht.

Der sichere Umgang mit R/3-Systemen setzt eine hochwertige Qualifikation und Spezialisierung voraus, die nur durch praktische Erfahrung, Fortbildung und einen stetigen Fluss von Informationen zu Sicherheitshinweisen, Fehlermeldungen etc. aufrechterhalten werden kann. Es sind also in der Berliner öffentlichen Verwaltung ebenso wie in den privaten Anwenderunternehmen alle Qualifikationsanstrengungen zu erbringen, die die sichere Beherrschung solcher Systeme überhaupt erst ermöglichen.

177 JB 1996, Anlage 6.1, Anlage 2 unserer Broschüre „Personal Computer und Datenschutz“, 1998

178 Der Leitfaden kann im Internet unter „http://www.sap-ag.de/germany/contact/user.htm“ mit der Bestellnummer 5002 4598 angefordert werden

5. Telekommunikation und Medien

5.1 Schichtenmodell im Telekommunikationsrecht

Das Telekommunikations- und Medienrecht hat in den vergangenen Jahren elementare Änderungen erfahren. Vor dem Hintergrund der *Liberalisierung der Telekommunikation,* die zu Beginn des vergangenen Jahres mit der endgültigen Beseitigung des staatlichen Monopols für *Telekommunikationsnetze* und *Sprachtelefonie* ihren Abschluss gefunden hat, sowie der stürmischen Entwicklung des Internets als globales elektronisches Kommunikationsmedium und der Intranets als unternehmens- oder behördeninternes Pendant, haben sich auch die rechtlichen Rahmenbedingungen erheblich fortentwickelt. Entstanden ist ein kompliziertes Regelungswerk, das dem Datenschutz erhebliche Bedeutung einräumt. Die zum ersten Mal im Berliner Bildschirmtexterprobungsgesetz von 1981 angelegten und später in der Telekommunikationsordnung und dem Bildschirmtextstaatsvertrag von 1986 fortentwickelten speziellen Datenschutzvorschriften durchdringen nun alle Bereiche der Telekommunikation – mit der Einfügung entsprechender Bestimmungen in den Rundfunkstaatsvertrag wird auch der Bereich der technischen Abwicklung des Rundfunks demnächst abgedeckt.

Das vergangene Jahr war geprägt von Bemühungen der Telekommunikationsanbieter, Diensteanbieter und Unternehmen und Behörden, die komplizierten und teilweise nicht widerspruchsfreien Bestimmungen in die Praxis umzusetzen.

Als schwierige Klippe stellte sich die Abgrenzung der einzelnen Regelungsbereiche heraus. Im Gegensatz zum gewohnten juristischen Denken, das bemüht ist, für bestimmte Sachverhalte jeweils *den,* aber auch nur *einen* geeigneten rechtlichen Rahmen zu finden, erfordert die Regelung der Telekommunikation ein Denken in *Schichten,* das in der Telekommunikationstechnik seit der Entwicklung moderner Netzstrukturen gängig ist. So unterscheidet das *Open Systems Interconnection (OSI) – Referenzmodell* der International Organization for Standardization (ISO) sieben übereinandergelagerte Schichten, deren Kommunikationsabläufe jeweils gesondert mit Hilfe von Kommunikationsprotokollen geregelt werden.

Die Schichten umfassen auf der untersten Ebene den physikalischen Vorgang der Signalübertragung, darübergelagert sind Übertragungssicherung und die Vermittlung im *Netz.* Während diese Vorgänge netzwerkabhängig sind und von denjenigen Stellen erbracht werden, die den Transport im Netz bewerkstelligen, richten sich die darübergelagerten Schichten an die Teilnehmer der Kommunikation selbst: Sie betreffen zum einen die Kommunikation zwischen den beteiligten Endgeräten, insbesondere die jeweilige Kommunikationsform, zum anderen die Darstellung und Verarbeitung des Inhalts der Informationen (Dienste-

schicht). Wichtig ist, dass bei jedem Telekommunikationsvorgang alle Schichten beteiligt sind, wenn auch möglicherweise mehr oder weniger ausgeprägt.

Eine adäquate juristische Regelung muss dieser Denkweise folgen, nur dann ist eine klare Abbildung rechtlicher und damit auch datenschutzrechtlicher Probleme auf die Architektur der Telekommunikation möglich.

Die deutsche Telekommunikationsgesetzgebung ist diesem Modell gefolgt, wenn auch die Schichten gebündelt werden und es eine Vielzahl von Unschärfen gibt, die auf die Entwicklung der Telekommunikation, aber auch auf eine bis heute noch nicht hinreichende theoretische Durchdringung der Materie zurückzuführen sind.

Das auf dem alten Fernmeldeanlagenrecht fußende *Telekommunikationsgesetz* (TKG) von 1996 richtet sich an die *Anbieter von Telekommunikationsdienstleistungen,* also an diejenigen Stellen, die für den „technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten“ (§ 3 Ziff. 16 TKG), mithin für die Abwicklung der unteren Schichten verantwortlich sind.

Die Anbieter von *Tele- und Mediendiensten,* die die besonderen Kommunikationsformen im Netz (e-mail, Surfen im Internet, Dateienabruf [file transfer, ftp]) ermöglichen, unterliegen dem Art. 1 (Teledienstegesetz [TDG]) und Art. 2 (Teledienstedatenschutzgesetz [TDDSG]) des IuK-Gesetzes von 1997[179] bzw. dem Mediendienste-Staatsvertrag. Dass die Sprachtelefonie als spezielle Kommunikationsform gleichwohl im Rahmen des TKG geregelt ist, gehört zu den historisch gewachsenen Unschärfen der Gesetzgebung.

Von der Dienstebene zu unterscheiden ist die Regelung der *Inhalte* selbst, und zwar deren Darstellungsform (Daten, Texte, Sprach- und Bildinformationen) und deren Verarbeitung. Hier greifen diejenigen Regelungen, die auch für die entsprechenden Inhalte außerhalb der Netze gelten *(„Offline-Recht“).*

Auch bei der rechtlichen Betrachtung der Telekommunikation gilt, dass stets alle drei Ebenen zu berücksichtigen sind: Das im vergangenen Jahr viel diskutierte Problem der Kinderpornografie im Internet[180] muss damit unter den Gesichtspunkten

- strafbarer Inhalte (StGB als Offline-Recht),
- der Verantwortlichkeit derjenigen Unternehmen, die den Zugang zu diesen Inhalten ermöglichen (Tele- bzw. Mediendiensterecht)
- und des Transports durch die Netze (TKG) betrachtet werden.

[179] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste – Informations- und Kommunikationsdienstegesetz vom 22. Juli 1997 (BGBl. I, S. 1870)

[180] vgl. 3.4

Auf der Ebene der Netze hat der Telekommunikationsanbieter wegen des *Fernmeldegeheimnisses* keine Eingriffsmöglichkeiten; hier müssen die Strafverfolgungsbehörden von ihren spezifischen Eingriffsbefugnissen (§§ 100 a ff. StPO, 88 TKG i.V.m. der Fernmeldeüberwachungsverordnung) Gebrauch machen.

Diese für Juristen ungewohnte Denkweise der Parallelgeltung verschiedener Regelungswerke stellt die Rechtsanwender vor erhebliche Probleme. Der Beratungsbedarf sowohl auf Seiten der Anbieter (Telekommunikationsunternehmen, Diensteanbieter und Gestalter inhaltlicher Angebote [„Content Provider“]) als auch auf Seiten der Unternehmen und Behörden als Nutzer ist erheblich. Auch die für die Kontrolle des Datenschutzes zuständigen Stellen (Bundesbeauftragter für den Datenschutz, Landesbeauftragte, Aufsichtsbehörden, Rundfunkbeauftragte) stehen vor großen Herausforderungen. Gerade der Berliner Datenschutzbeauftragte, der sich von Anfang an intensiv um Probleme des Datenschutzes bei der Telekommunikation bemüht hat, war hier in besonderer Weise gefordert.

Koordination der Datenschutzkontrolle im Telekommunikations-, Tele- und Mediendienstebereich

Die Überschneidung der Gesetzgebungsmaterien Telekommunikation sowie der Tele- und Mediendienste und die Verteilung der Datenschutzkontrollkompetenz in den jeweiligen Bereichen machen zur Sicherstellung einer bundesweit effizienten und gleichmäßigen Kontrolle eine verstärkte *Koordination* der beteiligten Aufsichtsbehörden erforderlich. Hier sind dem Berliner Datenschutzbeauftragten wichtige Aufgaben anvertraut worden: Zum einen ist uns durch den *„Düsseldorfer Kreis“* (das Koordinationsgremium der Aufsichtsbehörden für den Datenschutz im privaten Bereich) der Vorsitz der Arbeitsgruppe „Telekommunikations-, Tele- und Mediendienste“ des „Düsseldorfer Kreises“ übertragen worden; andererseits hat die Arbeit im bereits Ende 1997 vom Berliner Datenschutzbeauftragten eingerichteten *„Kooperationskreis IuK-Datenschutz“* – einem Koordinationsgremium, in dem neben dem Bundesbeauftragten für den Datenschutz, den Landesbeauftragten für den Datenschutz und den ministeriellen Aufsichtsbehörden für den privaten Bereich auch die unabhängigen Rundfunkdatenschutzbeauftragten sowie die Landesmedienanstalten vertreten sind – Tritt gefasst. Damit ist eine wesentliche Voraussetzung für eine gleichmäßige und koordinierte Anwendung der oben genannten Rechtsvorschriften gegeben.

Während der Vorsitz im deutschen Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten nach Brandenburg wechselte, behielt der Berliner Datenschutzbeauftragte den Vorsitz der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation (Interna-

tional Working Group on Data Protection in Telecommunications). Diese traf sich am 14./15. April 1998 in Hong Kong. In der sehr fruchtbaren Sitzung wurden gleich vier Beschlüsse verabschiedet: Grundsätze für datenschutzfreundliche Technologien im WWW, Gemeinsamer Standpunkt zum Datenschutz bei Suchmaschinen im Internet, Datenschutz bei invertierten Telefonverzeichnissen und Veröffentlichungspflichten beim Abhören privater Telekommunikation[181]. In der Sitzung am 9./10. November 1998 in Berlin wurden der Datenschutz bei den künftigen Verfahren der Domainnamenvergabe und bei der Verbreitung öffentlich zugänglicher Daten im Internet als künftige Beratungsthemen festgelegt.

5.2 Telekommunikationsnetze

Gesetzgebung

Umsetzung der ISDN-Richtlinie in das bundesdeutsche Recht

Die am 1. Dezember 1997 verabschiedete Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (früher ISDN-Richtlinie)[182] bestimmt in ihrem Artikel 15 Abs. 1 eine Umsetzungsfrist für die Mitgliedstaaten bis zum 24. Oktober 1998. Die Bundesregierung hat diese Frist verstreichen lassen, ohne die erforderlichen Anpassungen in der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV)[183] vorzunehmen. Wir haben gegenüber dem Bundesbeauftragten für den Datenschutz eine umfangreiche Stellungnahme mit Empfehlungen zur Novellierung der TDSV abgegeben. Über den sich aus der Richtlinie ergebenden Anpassungsbedarf hinaus sollte der Verordnungsgeber die Möglichkeit nutzen, die bereits im Bereich der Tele- und Mediendienste[184] niedergelegten Grundsätze der datensparsamen Gestaltung von Diensten auch auf den Telekommunikationsbereich auszuweiten. Neben der von uns in den zurückliegenden Jahren bereits mehrfach geforderten Einführung des „holländischen Modells", bei dem der angerufene Teilnehmer ein Wahlrecht erhält, ob seine Telefonnummer auf Einzelverbindungsnachweisen der Anrufenden ausgewiesen wird[185], sollte der Verordnungsgeber hier auch Rahmenbedingungen für den Einsatz datenschutzfreundlicher Technologien in der Telekommunikation[186] durch die Eröffnung der Möglichkeit der anonymen bzw. pseudonymen Nutzung auch von Telekommunikationsdiensten fördern.

181 Anlagenband „Dokumente zum Datenschutz 1998", Teil C
182 ABlEG Nr. L 241 vom 30. 1. 1998; vgl. JB 1997, 3.7.1
183 BGBl. I 1996, S. 982 ff.
184 vgl. JB 1997, 3.3 und 4.7.4
185 vgl. zuletzt JB 1997, 4.7.1
186 vgl. den Bericht des AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern (Hrsg.): Datenschutzfreundliche Technologien, Schwerin 1998

Verhältnis von Fernmeldegeheimnis zur Landesgesetzgebung und zu Dienst- und Betriebsvereinbarungen

Zur Frage, in welchem Verhältnis die Vorschriften über das Fernmeldegeheimnis nach § 85 TKG zur Landesgesetzgebung und zu Dienst- und Betriebsvereinbarungen stehen, hat der Kooperationskreis „IuK-Datenschutz" auf seiner Sitzung am 8. September 1998 folgende gemeinsame Position verabschiedet:

Die Vorschriften zum Schutz des Fernmeldegeheimnisses nach § 85 TKG beschränken den Umfang der vom geschäftsmäßigen Betreiber einer Telekommunikations-Nebenstellenanlage zulässiger Weise zu gewinnenden Erkenntnisse über Inhalt und nähere Umstände der Telekommunikation auf das für die Erbringung der Telekommunikationsdienste erforderliche Maß (§ 25 Abs. 3 TKG). Für landesgesetzliche Regelungen ist insoweit kein Raum. Die zulässigerweise gewonnenen Erkenntnisse sind zweckgebunden zu verwenden; Abweichungen von der Zweckbindung sind nur aufgrund einer gesetzlichen Vorschrift zulässig (§ 85 Abs. 3 Satz 3 TKG).

Betreiber von Telekommunikations-Nebenstellenanlagen (z. B. Arbeitgeber), die den Beschäftigten Telekommunikationsdienste zur *privaten* Nutzung zur Verfügung stellen, haben insoweit das Fernmeldegeheimnis zu wahren. Auswertungen über private Verbindungen sind auf das für eine Kostenerstattung unerlässliche Maß zu beschränken; weder durch Landesgesetz noch durch Dienst- oder Betriebsvereinbarung kann diese Beschränkung ausgeweitet werden.

Soweit Beschäftigte mit Hilfe einer Telekommunikations-Nebenstellenanlage *dienstlich* (d. h. durch den Arbeitgeber) veranlasste Telekommunikationsdienste in Anspruch nehmen, ist für den Einwirkungsbereich des Betreibers der Nebenstellenanlage der 11. Teil des TKG nicht unmittelbar anwendbar. Dem Betreiber (Arbeitgeber) bleibt daher ein Handlungsrahmen, in dem er unter ordnungsgemäßer Beteiligung der Arbeitnehmervertretung (Betriebs- bzw. Personalrat) und unter Berücksichtigung der bisherigen Rechtsprechung zum Arbeitnehmerdatenschutz Festlegungen (auch in Form von Dienst- oder Betriebsvereinbarungen) über Art und Umfang möglicher Auswertungen von Verbindungsdaten, u. U. aber auch von Telekommunikationsinhalten treffen kann.

Anwendung des § 90 TKG auf Nebenstellenanlagen in Krankenhäusern

Zur Frage, ob die Verpflichtung des § 90 TKG zur Führung von gesonderten Kundendateien und zur Bereithaltung dieser Dateien zum Online-Abruf durch die Regulierungsbehörde auch Nebenstellenanlagen in Krankenhäusern betrifft, hat der Kooperationskreis „IuK-Datenschutz" auf seiner Sitzung am 12./13. Februar 1998 folgende gemeinsame Position gefasst:

Die Pflicht zur Führung von *gesonderten* Kundendateien und zur Bereithaltung dieser Dateien zum Online-Abruf durch die Regulierungsbehörde nach § 90 TKG gilt nicht für Nebenstellenanlagen in Krankenhäusern, sondern lediglich für die Deutsche Telekom AG und ihre Konkurrenten auf dem liberalisierten Telekommunikationsmarkt. § 90 TKG verfolgt das Ziel, den Gerichten, Sicherheitsbehörden und Geheimdiensten auf dem liberalisierten Telekommunikationsmarkt auch bei einer Vielzahl von konkurrierenden Anbietern die Ermittlung eines bestimmten Anschlussinhabers zu ermöglichen, gegen den u. U. Maßnahmen der Telefonüberwachung angeordnet werden sollen. In der Monopolsituation im Sprachtelefondienst bis Ende 1997 war dies jedenfalls im Festnetz insoweit problemlos möglich, als die Deutsche Telekom AG zur Auskunft über jeden Hauptanschlussinhaber verpflichtet werden konnte. Auch bisher war es allerdings durch Online-Abruf beim Netzbetreiber möglich, die Namen von Patienten in Erfahrung zu bringen, die in einem bestimmten Zeitraum Nebenstellenanschlüsse eines Krankenhauses genutzt haben, weil die Deutsche Telekom AG über diese Informationen nicht verfügte. Der Bundesgesetzgeber wollte diesen Rechtszustand nicht ändern, sondern lediglich bei der Vielzahl jetzt konkurrierender Telekommunikationsunternehmen die Ermittlungsmöglichkeiten der Sicherheitsbehörden nicht einschränken. Für eine Erweiterung der Zugriffsmöglichkeiten über den bisherigen Rechtszustand hinaus besteht kein Anlass. Insbesondere wäre ein bundesweiter zentraler Zugriff auf Patientendateien neben der Krankenhausmeldepflicht (§ 16 Abs. 3 MRRG) unverhältnismäßig. § 90 TKG ist insoweit restriktiv auszulegen.

Überwachung des Telekommunikationsverkehrs

Für erhebliches Aufsehen in der Öffentlichkeit sorgte der im Juni 1998 öffentlich bekannt gewordene Entwurf des Bundeswirtschaftsministeriums für eine *Telekommunikations-Überwachungsverordnung* (TKÜV), die die veraltete Fernmeldeüberwachungsverordnung (FÜV) ersetzen sollte. Am Rande sei angemerkt, dass der im Juni lancierte Entwurf bereits vom Dezember des Vorjahres datierte und auch den Landesdatenschutzbeauftragten bis dahin nicht zugeleitet worden war. Wie bereits die Vorgänger-Verordnung FÜV soll die TKÜV regeln, welche technischen Maßnahmen Telekommunikationsanbieter zu treffen haben, um den so genannten „Bedarfsträgern“ (d. h. Strafverfolgungsbehörden und Nachrichtendiensten) die Überwachung des Telekommunikationsverkehrs ihrer Kunden technisch zu ermöglichen. Jedoch kann von einer einfachen Anpassung der Regelungen der alten Fernmeldeüberwachungsverordnung an die Bedingungen des liberalisierten Telekommunikationsmarktes keine Rede sein: Während sich die – gegenwärtig noch fortgeltende – Fernmeldeüberwachungsverordnung an Betreiber von Fernmeldeanlagen, die für den *öffentlichen* Verkehr bestimmt sind, richtet, sollte nach dem TKÜV-Entwurf vom Mai 1998

der Kreis der Verpflichteten auf alle Betreiber einer Telekommunikationsanlage ausgedehnt werden. Welche neue Dimension im Hinblick auf die überwachungsgerechte Anpassung der Telekommunikationsinfrastruktur damit erreicht wird, zeigt ein Blick in die Begriffsbestimmungen des Telekommunikationsgesetzes (TKG). Danach sind Telekommunikationsanlagen „. . . technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können[187]“. Darunter kann im Prinzip jede *Nebenstellenanlage* fallen, gleichgültig, ob diese lediglich zum eigenen Gebrauch betrieben oder Dritten zur Nutzung überlassen wird. Zwar schränkt der Entwurf selbst in § 20 den Kreis der Verpflichteten in gewisser Weise ein. Welche Haltung der Autoren diesem Entwurf zugrunde liegt, verdeutlicht jedoch eine Anmerkung im Entwurf der amtlichen Begründung in der Verordnung. Dort heißt es: „Künftig wird das Paket ‚technische Einrichtungen zur Überwachung der Telekommunikation‘ zum standardmäßigen Angebot einer Telekommunikationsanlage gehören.“ Selbstverständlich müssen solche Einrichtungen auf Kosten der Verpflichteten beschafft und betrieben werden.

Entsprechend groß war die Empörung in der Wirtschaft. Nachdem einige Unternehmen die ihnen durch die Vorhaltung technischer Einrichtungen und sicherheitsüberprüften Personals vermutlich entstehenden Kosten durchgerechnet hatten, ging ein Sturm der Entrüstung durch die Medienlandschaft, wie er in Fragen des Datenschutzes sonst nur selten zu verzeichnen ist. Daraufhin beraumte das aufgeschreckte Bundeswirtschaftsministerium eilig eine Anhörung für den Juni 1998 an, die eine Woche vor dem vorgesehenen Termin um einen Monat verschoben und dann in letzter Minute ersatzlos abgesagt wurde. Es ist davon auszugehen, dass der Kreis der Verpflichteten erheblich eingeschränkt werden wird. Gegebenenfalls sollte man auch vor einer Novellierung des auch aus anderen Gründen problematischen 11. Abschnitts des Telekommunikationsgesetzes (TKG) nicht zurückschrecken.

Im Gegensatz zur Überwachung der Inhalte der Telekommunikation nach §§ 100 a ff. StPO gestattet § 12 des Fernmeldeanlagengesetzes (FAG), der nach den verschiedenen Reformen des Telekommunikationsrechts noch als Torso des aus dem Jahre 1928 stammenden Gesetzes[188] übrig ist, eine nahezu unbeschränkte Übermittlung von *Verbindungsdaten* zur Strafverfolgung. Mehrfach hatten wir in den zurückliegenden Berichtsjahren die Ersetzung dieser Bestimmung durch eine verfassungskonforme Regelung in der Strafprozessordnung (StPO) angemahnt. Im Zuge der Beratungen für das „Begleitgesetz zum Telekommunikationsgesetz“ im Jahre 1997[189] hatte der Innenausschuss des

187 § 3 Nr. 17 TKG
188 RGBl. I, S. 8
189 vgl. JB 1997, 4.7.1

Bundestages die Bundesregierung aufgefordert, bis spätestens April 1998 eine verfassungskonforme Lösung zu finden, und eine Verlängerung des § 12 FAG über das Jahr 2000 explizit abgelehnt. Jedoch hat es die (alte) Bundesregierung wiederum versäumt, einen entsprechenden Vorschlag vorzulegen. Es steht zu hoffen, dass die Bundesregierung das Jahr 1999 nutzen wird, um diesen Zustand zu beenden.

Zum Ende des Berichtszeitraums hat das *Satellitentelefonnetz „Iridium",* das aus derzeit 66 Low-Earth-Orbit-Satelliten besteht, seinen Betrieb aufgenommen. Damit ist erstmals ein Dienst auf dem Markt verfügbar, der eine im Prinzip weltweite Erreichbarkeit unter einer einheitlichen Rufnummer unter Nutzung von Endgeräten ermöglicht, die hinsichtlich Abmessung und Gewicht den in den terrestrischen Mobilfunknetzen gebräuchlichen Handys entsprechen. Iridium ist ein Gemeinschaftsprojekt einer Investorengruppe, an dem unter anderem das Gemeinschaftsunternehmen von RWE und Veba, Otelo sowie Motorola und Kyocera beteiligt sind. Weitere vergleichbare Projekte anderer Konsortien sollen folgen.

Die Einführung solcher globalen Dienste wirft eine Reihe bisher ungelöster datenschutzrechtlicher Fragen auf: Während die bundesdeutschen Firmen, die Iridium in Zukunft vermarkten werden, hinsichtlich der Verarbeitung von Daten ihrer Kunden zweifelsfrei den bundesdeutschen Datenschutzbestimmungen des Telekommunikationsgesetzes und der dazu ergangenen Rechtsverordnung unterliegen werden, für deren Kontrolle der Bundesbeauftragte für den Datenschutz zuständig ist, können die für den Betrieb des Systems erforderlichen technischen Einrichtungen auch in solchen Ländern installiert werden, die über gar keine oder nur über unzureichende Datenschutzbestimmungen verfügen. Selbst die Koordination der Aufsichtsinstanzen in den Ländern, die über solche Kontrollgremien verfügen, dürfte in der Praxis erhebliche Schwierigkeiten aufwerfen. Völlig offen ist die Frage, wer für die Datenverarbeitung im Raumsegment verantwortlich ist und welche datenschutzrechtlichen Bestimmungen für diesen Teil der Verarbeitung gelten. Der einschlägige Weltraumvertrag[190] enthält keine diesbezüglichen Regelungen. Die derzeit weit reichendste *völkerrechtliche Regelung zum Schutz des Fernmeldegeheimnisses* enthält Artikel 37 des Internationalen Fernmeldevertrags, der im Rahmen der internationalen Fernmeldeunion geschlossen wurde. Artikel 37 des Internationalen Fernmeldevertrags verpflichtet die Mitglieder, „. . . alle nur möglichen Maßnahmen zu treffen, die mit dem verwendeten Fernmeldesystem vereinbar sind, um die Geheimhaltung der Nachrichten im internationalen Verkehr zu gewährleisten". Gleichzeitig behalten sich die Mitglieder jedoch das Recht vor, „. . . den zuständigen Behörden von diesem Nachrichtenverkehr Kenntnis zu geben, um die Anwendung ihrer innerstaatlichen Rechtsvorschriften oder die Ausführung internationaler Übereinkommen, deren Vertragspartner sie sind, zu sichern"[191]. Ob damit auch ein befriedigendes Schutzniveau für die Verarbeitung personenbezogener Daten bei der Telekommunikation im Raumsegment gewährleistet wird, ist offen.

Das Beispiel Satellitentelefonie verdeutlicht einmal mehr, dass der Schutz der Betroffenen durch nationales Recht allein im Zeitalter der globalen Telekommunikation nicht mehr zu gewährleisten ist.

Es kann kaum verwundern, dass die Globalisierung der Telekommunikationsinfrastruktur und die Einführung neuer satellitengestützter Dienste auch die Sicherheitsbehörden auf den Plan gerufen hat. Laut Presseberichten findet bereits mindestens seit 1996 eine internationale Kooperation zwischen den Staaten der Europäischen Union und den USA, Kanada, Norwegen, Australien und Neuseeland statt, bei der die Staaten auf ihrem jeweiligen Gebiet sicherstellen, dass Anbieter satellitengestützter Kommunikationssysteme den Sicherheitsbehörden einen Zugang zu den dort übertragenen Daten eröffnen[192].

Im September 1998 wurde ein Entwurf für eine Entschließung des Rates der Europäischen Union über die *rechtmäßige Überwachung des Telekommunikationsverkehrs in Bezug auf neue Technologien* öffentlich bekannt[193]. Dort wird unter Bezugnahme auf die Entschließung des Rates vom 17. Januar 1995 über rechtmäßige Überwachung von Telekommunikation[194] die Fortschreibung der dort festgelegten Anforderungen im Hinblick auf neue Technologien, wie beispielsweise mobile satellitengestützte Dienste und öffentliche auf IP basierende (Internet-) Dienste, vorgenommen. Im Wesentlichen wird dort gefordert, dass die Betreiber geeignete technische Maßnahmen treffen sollen, um eine lückenlose Überwachung des gesamten über die betreffenden Dienste übertragenen Datenvolumens im Hinblick auf bestimmte Benutzer durch die dazu ermächtigten Sicherheitsbehörden in Echtzeit zu ermöglichen. Auf das Fernmeldegeheimnis oder andere einschlägige Bestimmungen zum Schutz der Betroffenen wird in den Papieren überhaupt nicht Bezug genommen. Eine Erörterung von Datensicherheitsmaßnahmen erfolgt allerdings insofern, als die Betreiber sicherstellen sollen, dass die abgehörten Daten nur an die berechtigten Sicherheitsbehörden und nicht an unbefugte Dritte übertragen werden.

190 Vertrag über die Grundsätze zur Regelung von Tätigkeiten von Staaten bei der Erforschung und Nutzung des Weltraums einschließlich des Mondes und anderer Himmelskörper vom 27. Januar 1967, BGBl. 1996 II, S. 1969

191 vgl. BT-Drs. 13/3810 vom 16. Februar 1996 unter Ziff. 1841 f.

192 vgl. z. B. taz vom 18. 5. 1998, S. 3: „Auch der Lauschangriff geht in die Umlaufbahn"

193 vgl. http://www.heise.de/tp/deutsch/special/enfo/6326/1.html

194 vgl. ABlEG Nr. C 329, 4. Januar 1996, S. 1

Bedenklich erscheint insbesondere, dass hier offensichtlich unter Umgehung der nationalen parlamentarischen Kontrollgremien der Mitgliedstaaten eine *europa-, wenn nicht weltweite Infrastruktur geschaffen werden soll, die eine lückenlose Überwachung prinzipiell jedes Kommunikationsvorganges zulässt.* Darüber, welche gesellschaftlichen Risiken mit der Einrichtung derartiger Infrastrukturen verbunden sind, scheinen sich die Autoren keine Gedanken zu machen. Insofern gilt der Entwurf für die Ratsentschließung sogar noch über den deutschen Entwurf der TKÜV hinaus. Das Papier liest sich wie ein Wunschzettel der Sicherheitsbehörden. Da nicht zu erwarten ist, dass die Entschließung noch unter der jetzigen Ratspräsidentschaft verabschiedet werden wird, wird das Papier vermutlich im Jahre 1999 unter der dann deutschen Präsidentschaft weiter behandelt werden. Es steht zu hoffen, dass die Bundesregierung ihre Position dafür nutzen wird, hier einige Streben hinsichtlich der Sicherung des informationellen Selbstbestimmungsrechts der Teilnehmer am weltweiten Telekommunikationsverkehr einzuziehen.

Schon jetzt wird jedoch offensichtlich der internationale Telekommunikationsverkehr in großem Umfang durch die Geheimdienste anderer Staaten – namentlich der amerikanischen „National Security Agency (NSA)" – abgehört: In einem Bericht an das Europäische Parlament, der im Januar 1998 veröffentlicht wurde[195], wird auf das *globale Überwachungssystem „ECHELON"* hingewiesen, mit dem von verschiedenen Orten in Neuseeland, den USA, Australien, Hong Kong und Großbritannien die wichtigsten „Intelsat"-Satelliten abgehört werden, über die ein Großteil der satellitengestützten Telefongespräche, Internetverbindungen, E-Mails sowie Telefax- und Telexnachrichten abgewickelt wird. Dieses System ist offensichtlich in der Lage, anhand von Schlüsselwort-Katalogen, die in verschiedenen Sprachen vorliegen, aus dem globalen Datenstrom diejenigen Nachrichten herauszufiltern, die ein bestimmtes gesuchtes Schlüsselwort oder mehrere dieser Begriffe enthalten. Dem Bericht zufolge können neben der NSA offensichtlich auch entsprechende Stellen in den übrigen beteiligten Ländern auf diese Daten zugreifen. Unklar ist hingegen, für welche Zwecke die abgehörten Daten verwendet werden.

5.3 Tele- und Mediendienste

Evaluierung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)

Bei der Verabschiedung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) im Jahr 1997 hatte der Bundestag der Bundesregierung eine Evaluierung der neuen Regelungen innerhalb

[195] European Parliament / Directorate General for Research/ Directorate B / The STOA Programme (Hrsg): An Appraisal of Technologies of Political Control, 19. Januar 1998, Dok.-Nr.: PE 166 499/ Int. St.

eines Zeitraumes von zwei Jahren nach In-Kraft-Treten des Gesetzes auferlegt[196]. Mit dem Neuzuschnitt der Ressorts in der Folge der Bundestagswahl ist die Zuständigkeit für die Evaluierung des IuKDG unterdessen vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie zum Bundesministerium für Wirtschaft verlagert worden. Im zurückliegenden Zeitraum konzentrierte sich die Evaluierungsdiskussion überwiegend auf Fragen der Anbieterverantwortung für Inhalte von Internet-Angeboten[197].

Das *Teledienstedatenschutzgesetz* (TDDSG; Artikel 2 des IuKDG) hat sich in der Praxis der Datenschutzbeauftragten und der Aufsichtsbehörden überwiegend bewährt. Bestehende Anwendungsprobleme des Telekommunikations-, Mediendienste- und Teledienstrechts werden fortlaufend in enger Kooperation der Datenschutzbeauftragten des Bundes und der Länder, der Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich sowie der Rundfunkdatenschutzbeauftragten und der Datenschutzbeauftragten der Landesmedienanstalten geklärt.

Im Hinblick auf die zunehmende Internationalisierung der Teledienste im Zusammenhang mit dem aufkommenden „Global Electronic Commerce" wäre es jedoch sinnvoll, wenn das bereits jetzt in § 17 des Mediendienste-Staatsvertrages (MDStV) vorgesehene *Datenschutz-Audit* auch in das TDDSG aufgenommen würde. Dies gilt insbesondere vor dem Hintergrund der Bemühungen verschiedener – vor allem in den USA ansässiger – Anbieter zur Datenschutzzertifizierung von Angeboten im Internet[198]. Im Rahmen eines Datenschutz-Audits könnten Qualitätsnormen definiert und umgesetzt werden, die datenschutzkonformen deutschen Angeboten und Anbietern auch auf internationaler Ebene ein Wettbewerbsvorteil verschaffen könnten.

In der Praxis hat es sich zunehmend als Problem herausgestellt, dass im Internet eine sichere Authentifizierung von Anbietern und Nutzern von Telediensten nicht in ausreichendem Maße gewährleistet ist. Dass im Internet eine Vertraulichkeit der Datenübertragung nicht generell sichergestellt ist, ist ein weiteres Hindernis für die geschäftliche Nutzung. Aus diesem Grunde sollten Projekte zur Entwicklung von *Sicherheitsinfrastrukturen* – auch mit öffentlichen Mitteln – verstärkt gefördert werden. In diesem Zusammenhang käme Projekten, die die Umsetzung des Gebotes zur Datensparsamkeit nach § 3 Abs. 4 TDDSG zum Gegenstand haben, besondere Bedeutung zu, insbesondere aber solchen Projekten, die sich mit Möglichkeiten der anonymen und pseudonymen Nutzung des Internet befassen.

Das TDDSG sollte analog den Vorschriften des § 20 MDStV um einen Ordungswidrigkeitenkatalog ergänzt werden.

[196] BT-Drs. 13/7935 vom 11. 6. 1997
[197] vgl. dazu 3.4
[198] vgl. JB 1997, 3.3 zu „PICS" und „P3P"

Vor dem Regierungswechsel war in der Presse verschiedentlich über Pläne des Bundesinnenministeriums berichtet worden, bei einer eventuellen Novellierung des Teledienstegesetzes die Anbieter von Telediensten dazu zu verpflichten, den Sicherheitsbehörden Bestandsdaten ihrer Kunden zu übermitteln oder diese – analog den jetzt geltenden Regelungen des § 90 TKG – sogar elektronisch zum Abruf bereitzuhalten. Derartige Bestrebungen konnten sich bereits während des Gesetzgebungsverfahrens zum IuKDG aus guten Gründen nicht durchsetzen; die Einführung solcher Verpflichtungen für die Anbieter wird von uns nach wie vor entschieden abgelehnt. Es steht zu hoffen, dass die neugewählte Bundesregierung dieses Vorhaben nicht weiterverfolgen wird.

Geltung des Fernmeldegeheimnisses für Anbieter von Tele- und Mediendiensten

Zu dieser Frage vertritt der Kooperationskreis „IuK-Datenschutz" die Auffassung, dass das Fernmeldegeheimnis auch Anbieter von Telediensten bindet. Das Teledienstegesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Zeichen bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt (§ 2 Abs. 1 TDG). Sowohl das Teledienstegesetz als auch das Teledienstedatenschutzgesetz setzen an mehreren Stellen die Geltung des Fernmeldegeheimnisses für Anbieter von Telediensten voraus (vgl. § 5 Abs. 4 TDG; § 6 Abs. 4 Satz 2 TDDSG). Der Diensteanbieter hat außerdem durch technisch-organisatorische Vorkehrungen u. a. sicherzustellen, dass der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann (§ 4 Abs. 2 Nr. 3 TDDSG). Das gesamte Teledienstedatenschutzgesetz enthält detaillierte Restriktionen für die Verwendung nutzerbezogener Daten durch Diensteanbieter. Allerdings unterliegen dem Fernmeldegeheimnis in erster Linie *Nutzungs- und Abrechnungsdaten* (wie auch – z. B. bei E-Mail – Inhaltsdaten, deren Verwendung im IuKDG nicht geregelt ist), nicht aber Bestandsdaten. Das Fernmeldegeheimnis, das seine Grundlage in Art. 10 des Grundgesetzes und § 85 TKG hat, ragt insoweit von der Ebene des Telekommunikationsrechts aus auch in die durch TDG und TDDSG geregelte Diensteebene hinein. Der Schutz des Fernmeldegeheimnisses beschränkt sich somit nicht auf die Ebene des physikalischen Netzes.

Erhebung und Verarbeitung von Nutzungs- und Abrechnungsdaten bei Tele- und Mediendiensten auf der Grundlage der Einwilligung

Verschiedentlich wurde die Frage aufgeworfen, ob auf der Grundlage der Einwilligung der Betroffenen auch Nutzungs- und Abrechnungsdaten über das in § 6 TDDSG bzw. § 5 MDStV genannte Maß hinaus verarbeitet werden dürfen. Die Arbeitsgruppe „Telekommunikations-, Tele- und Mediendienste" des Düsseldorfer Kreises vertritt hierzu die Auffassung, dass auf der Grundlage der Einwilligung auch Nutzungs- und Abrechnungsdaten über das in den betreffenden Rechtsvorschriften genannte Maß hinaus verarbeitet werden dürfen, obwohl dies in den jeweiligen Paragraphen – im Gegensatz zu den entsprechenden Bestimmungen über Bestandsdaten – nicht ausdrücklich erwähnt ist. Allerdings sind auch an die Einwilligung inhaltliche Maßstäbe anzulegen, insbesondere der Erforderlichkeit der Daten für den jeweiligen Zweck.

Geltung des TDDSG für geschlossene Benutzergruppen und Verhältnis zu den Regelungen des § 10 BDSG

In der Arbeitsgruppe des Düsseldorfer Kreises wurde darüber hinaus erörtert, ob in Fällen, in denen ein Unternehmen den Zugriff auf seine Datenbestände für externe Kunden öffnet, das Teledienste-Recht durch die Regelungen des § 10 BDSG über die Einrichtung automatisierter Abrufverfahren verdrängt wird. Beim Angebot derartiger Dienste handelt es sich nach überwiegender Auffassung um Teledienste im Sinne des TDG.

Allerdings ist nach Auffassung der Arbeitsgruppe in diesen Fällen eine Protokollierung über die Regelungen des TDDSG hinaus im Rahmen der Bestimmungen des § 10 BDSG möglich. Insbesondere § 10 Abs. 4 BDSG ist insofern als „andere Rechtsvorschrift" im Sinne des § 3 Abs. 1 TDDSG anzusehen. Dies gilt allerdings nur für geschlossene Benutzergruppen, da § 10 Abs. 5 die Anwendung der übrigen Absätze des § 10 BDSG für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen, ausschließt.

Geltung von TDDSG und MDStV im Arbeitsverhältnis

Zu den wesentlichen Problemen der Anwendung von TDDSG und MDStV gehört die Frage, inwieweit diese Bestimmungen im Arbeitsverhältnis Anwendung finden können. Dies hätte unter anderem zur Folge, dass der Arbeitgeber (als Teledienstеanbieter) den Arbeitnehmern (als Nutzern von Telediensten) im Regelfall die anonyme bzw. pseudonyme Nutzung dieser Dienste ermöglichen müsste. Zu den Tele- bzw. Mediendiensten gehört beispielsweise das World Wide Web (WWW), das sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft eine immer größere Verbreitung findet.

Nach der in der Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste" des „Düsseldorfer Kreises" sowie im „Düsseldorfer Kreis" selbst abgestimmten Auffassung sind jedoch *Arbeitgeber nicht als Tele- bzw. Mediendiensteanbieter* anzusehen, soweit den Arbeitnehmern ausschließlich die dienstliche Nutzung der zur Verfügung gestellten Dienste gestattet und eine private Nutzung ausdrücklich ausgeschlossen ist. Dabei soll es keinen Unterschied machen, ob dem Arbeitnehmer lediglich unternehmensintern zur Verfügung gestellte Tele- bzw.

Mediendienste zugänglich gemacht werden oder ob auch auf Angebote Dritter (z. B. über das Internet) zugegriffen werden kann. TDG und MDStV setzen voraus, dass es sich bei Diensteanbieter und Nutzer um zwei verschiedene Instanzen handelt. Dies ist bei Diensten, die dem Arbeitnehmer durch den Arbeitgeber zur dienstlichen Nutzung zur Verfügung gestellt werden, nicht der Fall (In-sich-Verhältnis).

Ist dagegen eine private Nutzung der Tele- bzw. Mediendienste zugelassen, so gelten hinsichtlich dieser privaten Nutzung für den Arbeitgeber die Vorschriften des TDG/TDDSG bzw. des MDStV in vollem Umfang. In diesem Fall muss technisch eine *Unterscheidung der privaten und dienstlichen Nutzung* der Tele- bzw. Mediendienste möglich sein. Ist eine solche Unterscheidung nicht möglich, so sind die Vorschriften von TDG/TDDSG bzw. MDStV auf die gesamte (also auch auf die dienstliche) Nutzung der Dienste anwendbar.

Die Protokollierung der dienstlichen Nutzung von Tele- bzw. Mediendiensten durch den Arbeitgeber ist allgemein im Rahmen der arbeitsrechtlichen Erfordernisse („offline-Recht“) gestattet. Diese müssen jedoch in jedem Einzelfall geprüft werden. Jedenfalls ist eine Vollprotokollierung aller Einzelzugriffe eines Arbeitnehmers im World Wide Web unverhältnismäßig. Bei der Auswertung von Nutzungsdaten über die dienstliche Nutzung von Diensten ist darüber hinaus § 31 BDSG zu beachten, der für solche Daten eine besonders strenge Zweckbindung vorsieht. Darüber hinaus sind sowohl Protokollierung als auch Auswertung von Nutzungsdaten zweifelsfrei mitbestimmungspflichtig.

Die Protokollierung der privaten Nutzung von Tele- bzw. Mediendiensten durch den Arbeitnehmer ist dagegen grundsätzlich nicht gestattet, soweit sie nicht für Abrechnungszwecke erforderlich ist oder der Betroffene eingewilligt hat[199]. Eine Auswertung von Protokollen, die im Rahmen der Einwilligung des Arbeitnehmers erstellt werden, ist ebenfalls nur im Rahmen dieser Einwilligung gestattet. Davon unberührt bleiben die Protokollierungsbefugnisse, die sich aus der Verpflichtung zu Maßnahmen der Datensicherung nach § 9 BDSG ergeben. Diese Daten dürfen allerdings nur zu diesen Zwecken genutzt werden[200].

Private und dienstliche Nutzung von E-Mail im Arbeitsverhältnis

Auch bei der Nutzung von E-Mail-Diensten ist mit dem Obengesagten eine Unterscheidung der verschiedenen Nutzungsformen erforderlich. Diese kann beispielsweise dadurch sichergestellt werden, dass den Beschäftigten zur Unterscheidung der verschiedenen Nutzungsformen unterschiedliche E-Mail-Adressen zugeordnet werden, aus denen sich der dienstliche bzw. private Charakter der Adresse ergibt.

199 §§ 6 Abs. 1 Nr. 2 i.V.m 3 Abs. 1 TDDSG; 15 Abs. 1 Nr. 2 i.V.m 12 Abs. 3 MDStV
200 §§ 14 Abs. 4, 31 BDSG; § 11 Abs. 5 BlnDSG

Der Arbeitgeber darf einzelne dienstliche E-Mails auch dann einsehen, wenn sie an einen bestimmten Arbeitnehmer gerichtet sind. Der Arbeitnehmer hat dem Arbeitgeber den Zugang zu solchen E-Mails zu eröffnen. Dagegen ist eine *Auswertung des gesamten E-Mail-Verkehrs* (etwa durch automatisches „Scannen“) durch den Arbeitgeber jedenfalls im Regelfall nicht gestattet. Besondere Regelungen gelten für spezielle Vertrauensbereiche in Betrieben, so z. B. für E-Mails, die an den Betriebsrat oder den betrieblichen Datenschutzbeauftragten gerichtet sind oder von diesen versandt werden.

Soweit eine private Nutzung von E-Mail-Diensten durch die Arbeitnehmer gestattet ist, gilt hinsichtlich der Inhaltsdaten der E-Mails sowie der Verbindungsdaten das *Fernmeldegeheimnis,* das durch den Arbeitgeber zu wahren ist. Der Arbeitgeber darf daher grundsätzlich nicht vom Inhalt privater E-Mails, die von Beschäftigten herrühren oder an ihn gerichtet sind, Kenntnis nehmen. Dies gilt auch, soweit ein Verdacht auf strafbare Handlungen besteht. In diesem Fall muss der Arbeitgeber die Staatsanwaltschaft einschalten, die dann im Rahmen ihrer Befugnisse nach der Strafprozessordnung die Daten der Beschäftigten einsehen kann.

Mitarbeiterdaten im Internet

Öffentliche Stellen des Landes Berlin gehen zunehmend dazu über, Daten ihrer Mitarbeiter (z. B. Name, Sachgebiet, Raumnummer, Telefonnummer etc.) auch im Internet zu veröffentlichen. Dagegen hatte ein Mitarbeiter einer öffentlichen Stelle gegenüber seinem Dienstherrn Widerspruch erhoben und eine Streichung seines Namens aus dem Internet-Angebot der Behörde gefordert. Nachdem dieses Anliegen mit der Dienststellenleitung nicht befriedigend geklärt werden konnte, wandte sich der Mitarbeiter an uns mit der Bitte um datenschutzrechtliche Überprüfung.

Über Aspekte des Datenschutzes bei der Veröffentlichung der Mitarbeiterdaten im Internet durch öffentliche Stellen des Landes Berlin hatten wir bereits in unserem Jahresbericht 1997 berichtet[201]. Zu den dort formulierten Grundsätzen gehörten neben einer Beschränkung auf die Veröffentlichung von Basiskommunikationsdaten von Arbeitnehmern, die Information der Arbeitnehmer und die Beschränkung der Veröffentlichung personenbezogener Daten auf Funktionsträger (zu denen z. B. der Pförtner und das Reinigungspersonal zweifelsfrei nicht zählen). Darüber hinaus hatten wir wegen der besonderen Gefährdung des informationellen Selbstbestimmungsrechts der Mitarbeiter bei einer weltweiten Veröffentlichung ihrer Daten – nämlich auch in solchen Ländern, in denen überhaupt kein oder jedenfalls kein hinreichender Datenschutz besteht – empfohlen, den Betroffenen grundsätz-

201 vgl. JB 1997, 4.7.3

lich eine Widerspruchsmöglichkeit gegen die Aufnahme ihrer Daten in öffentliche elektronische Verzeichnisse einzuräumen. In solchen Fällen könnte der Name beispielsweise durch das Stellenzeichen oder Ähnliches ersetzt werden.

Zwar hat die betroffene Dienststelle zunächst darauf hingewiesen, dass für eine zukunfts- und bürgerorientierte Gestaltung der Verfahren in der öffentlichen Verwaltung auch die Veröffentlichung von Mitarbeiterdaten im Internet unumgänglich sei; letztendlich konnten wir die betreffende Behörde davon überzeugen, *Widersprüche der Mitarbeiter* im Einzelfall zu akzeptieren und umzusetzen.

Auch der Senat von Berlin hat zu unseren Ausführungen über die Veröffentlichung von Mitarbeiterdaten im Internet Stellung genommen[202]. Leider wird dort der Schluss gezogen, dass gegen eine Veröffentlichung von Mitarbeiterdaten im Internet schon allein deswegen nichts einzuwenden sei, weil deren Daten bereits jetzt in gedruckten Telefonverzeichnissen über öffentliche Bibliotheken des Landes Berlin zugänglich sind. Diese Auffassung verkennt, dass im Gegensatz zu gedruckten Verzeichnissen elektronische Mitarbeiterverzeichnisse weltweit elektronisch ausgewertet und ggf. mit anderen Daten zusammengeführt werden können. Im konkreten Einzelfall kann daher eine erhöhte Gefährdung des informationellen Selbstbestimmungsrechts der Mitarbeiter jedenfalls nicht ausgeschlossen werden. Eine Gleichsetzung elektronischer und gedruckter Verzeichnisse ist nicht sachgerecht.

5.4 Datenschutz und Medien

Vierter Rundfunkänderungsstaatsvertrag

Auch im zurückliegenden Berichtszeitraum ist der Vierte Rundfunkänderungsstaatsvertrag, mit dem unter anderem die Einführung des digitalen Fernsehens reguliert werden soll, nicht verabschiedet worden. Nach den uns vorliegenden Informationen besteht nach wie vor ein Dissens zwischen den Ländern über Einzelheiten der Finanzierung der ARD.

Dagegen sind die Datenschutzbestimmungen des Entwurfs für den Vierten Rundfunkänderungsstaatsvertrag, die von den Rundfunkreferenten der Länder in Abstimmung mit Vertretern der Landesdatenschutzbeauftragten gestaltet worden sind, weitgehend unumstritten. Aus Sicht der Datenschutzbeauftragten kommt es bei der *Regulierung des digitalen Fernsehens* vor allem darauf an, die Gestaltung der technischen Einrichtungen an dem Ziel auszurichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden *(Prinzip der Datensparsamkeit)*. Die Rundfunkveranstalter sollen

[202] vgl. Abghs.-Drs. 13/2981, S. 124 f.

verpflichtet werden, die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn der Benutzer ausdrücklich einen Einzelnachweis verlangt. Insgesamt sollen die Datenschutzbestimmungen des Rundfunkstaatsvertrages mit denen des bereits existierenden Mediendienste-Staatsvertrages von 1997 harmonisiert werden, um für Mediendienste und Rundfunk einen gleichmäßigen – hohen – Datenschutzstandard sicherzustellen. In diesem Zusammenhang sollte auch das bereits im Mediendienste-Staatsvertrag enthaltene *Instrument des „Datenschutz-Audits",* bei dem Veranstalter ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen können, eingeführt werden.

Umso bedenklicher müssen Pressemeldungen stimmen, nach denen große potentielle Anbieter des digitalen Fernsehens – insbesondere die Kabelfernseh-Tochter der Deutschen Telekom AG – den Einsatz der *D-Box der Kirch-Gruppe* als Standard-Decoder für digitale Sendungen im Kabelnetz befürworten. Nach unserem Kenntnisstand lässt die D-Box derzeit eine anonyme bzw. pseudonyme Nutzung der neuen digitalen Dienste nicht zu. Es sind allerdings sehr wohl technische Alternativen am Markt vorhanden, mit denen dies möglich wäre.

Vor diesem Hintergrund hat die 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 19./20. März 1998 eine Entschließung zum Datenschutz beim digitalen Fernsehen gefasst, in dem nochmals die immense Bedeutung der datenschutzgerechten Gestaltung dieser neuen Dienste betont wird[203]. Die Rundfunkveranstalter und Hersteller sollten die Anforderungen des Datenschutzes schon jetzt bei der Planung und Gestaltung von digitalen Angeboten berücksichtigen.

Rundfunk-Staatsvertrag Berlin-Brandenburg

Am 3. November 1998 wurde der Erste Staatsvertrag zur Änderung des Staatsvertrages über die Zusammenarbeit der Länder Berlin und Brandenburg im Bereich des Rundfunks abgeschlossen. Der Staatsvertrag ist unterdessen in Kraft getreten.

Der Änderungsstaatsvertrag ist durch das Gesetz zu dem Ersten Staatsvertrag zur Änderung des Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks[204] in geltendes Berliner Landesrecht überführt worden.

[203] Anlagenband „Dokumente zum Datenschutz 1998"
[204] GVBl. 1998, S. 406 ff.

Ziel der Änderung des Staatsvertrages war die Anpassung der Vorschriften an den Dritten Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge sowie den Staatsvertrag über Mediendienste.

Die Änderung des Staatsvertrages zwischen Berlin und Brandenburg betrifft unter anderem auch die Datenschutzvorschriften: Hinsichtlich der Inhalte von Rundfunkdarbietungen ist die Vorschrift über unzulässige Sendungen um eine an die *„Reality-TV-Vorschrift“* des Rundfunkstaatsvertrages[205] angelehnte Regelung ergänzt worden, nach der Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, nicht in einer die Menschenwürde verletzenden Weise dargestellt oder ein tatsächliches Geschehen wiedergegeben werden darf, ohne dass ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt. Die Einwilligung der Betroffenen ist in diesem Fall unbeachtlich[206].

Die Vorschrift über die *Datenschutzkontrolle* im Geltungsbereich des Medienstaatsvertrags Berlin – Brandenburg ist in der Weise geändert worden, dass künftig nur noch länderübergreifende gemeinsame Einrichtungen von dem Berliner Datenschutzbeauftragten im Einvernehmen mit der im Land Brandenburg zuständigen Kontrollbehörde überwacht werden. Ansonsten gilt auch hier das Sitzland-Prinzip[207].

Aus Datenschutzsicht wird sich mit der Verabschiedung des Vierten Rundfunkänderungsstaatsvertrages für den Medienstaatsvertrag Berlin-Brandenburg erneut ein Änderungsbedarf ergeben: So müssen insbesondere die dort vorgesehenen Verpflichtungen der Diensteanbieter zu anonymen oder pseudonymen Angeboten von Rundfunkdiensten und zur datensparsamen Gestaltung dieser Dienste auch in die in Berlin und Brandenburg geltenden Bestimmungen übernommen werden.

6. Berliner Datenschutzbeauftragter

6.1 Die Dienststelle

Der langjährige Stellvertreter des Berliner Datenschutzbeauftragten für den Bereich Recht, Dr. Alexander Dix, wurde am 25. März 1998 zum Nachfolger von Dr. Dietmar Bleyl gewählt, der sechs Jahre das Amt des Landesbeauftragen für den Datenschutz des Landes Brandenburg innehatte. In dieser Zeit gab es eine Vielzahl von Kontakten, beginnend von Hilfestellungen beim Aufbau der Dienststelle bis hin zu regelmäßigen Bemühungen, die Arbeit in beiden Ländern zu koordinieren. Dem

205 vgl. § 3 Abs. 1 Nr. 5 des Rundfunkstaatsvertrages (RStV) vom 31. August 1991, zuletzt geändert durch § 22 des Staatsvertrages vom 1. August 1997 (GVBl. 1997, S. 366)
206 vgl. § 48 Abs. 1 Nr. 7 des Ersten Staatsvertrages zur Änderung des Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks
207 vgl. § 58 Abs. 8 des Ersten Staatsvertrages zur Änderung des Staatsvertrages über die Zusammenarbeit zwischen Berlin und Brandenburg im Bereich des Rundfunks

Engagement von Dr. Bleyl verdanken wir manche Einsichten in die Probleme, denen sich der Datenschutzbeauftragte in einem neuen Bundesland gegenübersieht und die nicht wie im Falle von Berlin durch eine Verschränkung der Verwaltungen von Anfang an gedämpft worden sind.

Dr. Dix übernimmt als erster Datenschutzbeauftragter neben seiner ursprünglichen Aufgabe auch die Aufgabe des Landesbeauftragten für die Akteneinsicht wahr. Für die Gewährung der allgemeinen Akteneinsicht in die Unterlagen der öffentlichen Verwaltung ist das Land Brandenburg bahnbrechend[208]; es geht, abgestützt durch eine ebenso wegweisende Verfassungsbestimmung[209], dem Bund und den anderen Ländern in einer weltweiten Entwicklung voran, die 1766 in Schweden vorweggenommen worden war und in einer Reihe von Staaten unter dem Begriff der „Informationsfreiheit“, von den USA im Jahr 1967 bis jüngst in Irland im Jahr 1997, Nachahmer gefunden hat. Auch das Modell, den Datenschutzbeauftragten und den Informationsfreiheitsbeauftragten unter einem Dach zu vereinen, hat Vorläufer in einigen Provinzen Kanadas und Ungarn. Sollte es in Berlin zu einer entsprechenden Gesetzgebung kommen, sollte ebenfalls dieses Modell angestrebt werden – es würde den Datenschutz auch von dem (falschen) Ruf befreien, einseitig nur die Verhinderung des Zugangs zu Daten zu betreiben.

Der Wechsel von Dr. Dix, dessen Einsatz die Dienststelle viel zu verdanken und der ihr mit zu internationalem Renommee verholfen hat, wurde zum Anlass genommen, eine Straffung der internen Organisation der Dienststelle vorzunehmen. Die beiden bisher bestehenden juristischen Bereiche wurden zusammengelegt, besondere Querschnittsaufgaben (Internationaler Datenschutz, Datenschutz in der Telekommunikation, Arbeitnehmerdatenschutz) im Zentralen Bereich unter Leitung des Datenschutzbeauftragten konzentriert[210]. Verbunden wurde dies mit Bemühungen, auch in unserer Dienststelle trotz ihrer geringen Größe die Grundideen der Verwaltungsreform umzusetzen[211].

Die Verteilung der neuen Vorgänge auf die einzelnen Arbeitsgebiete ist seit vielen Jahren in etwa gleich bleibend: An der Spitze stehen mit nahezu gleich vielen Vorgängen die Bereiche Inneres und Gesundheit/Soziales, gefolgt von Fällen aus den Bereichen Wirtschaft, Justiz und Bildung.

Nach wie vor als erschwerend stellt sich heraus, dass der Dienststelle kein eigener Dienstwagen mehr zur Verfügung steht; ein entsprechender Antrag im Abgeordnetenhaus wurde erneut abgelehnt. Für eine

208 vgl. 1.2
209 Art. 21 Abs. 4 Verfassung des Landes Brandenburg
210 vgl. den Geschäftsverteilungsplan, Anlage Nr. 2
211 vgl. 6.2

Dienststelle, die über den ganzen Landesbereich hinweg mit derart wenigen Mitarbeitern Prüfungen vor Ort, in manchen Fällen auch spontan, vornehmen muss, ist es nicht nur unbequem, sondern beeinträchtigt auch die effektive Aufgabenerfüllung, wenn nicht die Möglichkeit besteht, über ein jederzeit einsetzbares Kraftfahrzeug zu verfügen. Die – zunehmend schwierigere – Nutzung des Fuhrparks, öffentlicher Verkehrsbetriebe oder auch von Taxis schafft hier keinen Ersatz.

Wiederum haben sich Mitarbeiterinnen und Mitarbeiter der Dienststelle in den verschiedensten Einrichtungen intensiv um Aus- und Fortbildung von Dienstkräften der Verwaltung und von Studenten und Schülern bemüht, in einer Vielzahl von Vorträgen wurden verschiedenste Interessengruppen über die Belange des Datenschutzes informiert.Wieder wurden viele Gäste betreut, die sich bei uns über den Datenschutz in Berlin und darüber hinaus in Deutschland und Europa unterrichten wollten.

6.2 Verwaltungsreform

Unsere eigene Organisation und Arbeitsweise muss in hinreichender Weise flexibel und dynamisch gestaltet sein, um auf die quantitativen und vor allem die qualitativen Veränderungen innerhalb unseres Betätigungsfeldes vorbereitet zu sein. Aus diesem Grunde haben wir im Berichtsjahr eine interne Organisationsüberprüfung vorgenommen, die sich sowohl auf die Aufbau- als auch die Ablauforganisation richtete[212]. Hierbei haben wir uns an Elemente und Vorgehensweisen der Berliner Verwaltungsreform angelehnt, soweit diese Ansätze auf eine Kontroll- und Aufsichtsbehörde wie den Datenschutzbeauftragten übertragen werden können.

Nachdem die Mitarbeiterinnen und Mitarbeiter der Dienststelle über Grundzüge und Elemente der Reform informiert wurden und eine Zeit- und Maßnahmeplanung erarbeitet war, bildete eine Bestandsaufnahme und Analyse der Ist-Situation die Grundlage des weiteren Vorgehens. Hierbei wurden sowohl die Bearbeitungsprozesse (in einer „Prozess- und Schnittstellenanalyse“) als auch die Verwaltungsergebnisse (in qualifizierten „Produktbeschreibungen“) in den Blick genommen.

Die Prozess- und Schnittstellenanalyse richtete sich dabei auf die wesentlichen Geschäftsvorgänge und deren Bearbeitung. Schwerpunkt der Untersuchung war die Bearbeitung von Bürgereingaben. Dabei wurden zunächst sämtliche Teilschritte eines hierfür typischen Bearbeitungsprozesses erfasst und strukturiert ihrem Verlauf folgend abgebildet. Dies lieferte die Grundlage, anhand einer festgelegten Stichprobengröße die durchschnittlichen Bearbeitungs- und Liegezeiten der einzelnen Teilbearbeitungsschritte zu ermitteln. Unter der Zielsetzung, die Bearbeitungszeiten insgesamt zu verkürzen, wurden hinsichtlich der internen Abläufe Maßnahmen zur Straffung des Bearbeitungsverfahrens eingeleitet.

Über die internen Abläufe hinaus wurden jedoch auch die Schnittstellen zu speichernden Stellen in die Untersuchung einbezogen, soweit diese zur Stellungnahme über die uns vorgetragenen Sachverhalte aufgefordert wurden. Diese Betrachtung brachte Ergebnisse zutage, die in der Tendenz zwar erwartbar, in ihrer Ausprägung allerdings überraschend, ja alarmierend sind: Bei der Bearbeitung von Bürgereingaben, die sich auf Vorfälle und Vorgänge in der öffentlichen Verwaltung beziehen, macht die Zeit des bloßen Wartens auf den Eingang von Stellungnahmen der betreffenden Behörden zwei Drittel (67 %) der Gesamtbearbeitungsdauer des Vorgangs aus. Bei privatwirtschaftlichen Organisationen beträgt dieser Anteil demgegenüber lediglich ein knappes Drittel (31 %). Während uns Stellungnahmen aus dem privaten Bereich durchschnittlich nach 25,2 Tagen vorliegen, benötigt die Verwaltung hierfür im Schnitt 96,9 Tage – fast viermal so lange. Diese Zahlen zeigen deutlich unser Dilemma: Entweder durch den Verzicht auf die Einholung von Stellungnahmen zwar schneller, aber mit einem geringeren Wirkungsgrad zu arbeiten, oder aber um den Preis einer längeren Bearbeitungsdauer unmittelbarere Verbesserungen des Datenschutzes zu erreichen.

Grundlage der Analyse der Verwaltungsergebnisse des Berliner Datenschutzbeauftragten war die Erarbeitung eines behördlichen Produktkataloges. In einem ersten Schritt wurden für die einzelnen Produkte in Arbeitsgruppen Qualitätsziele und Qualitätsindikatoren gebildet, deren Abstimmung derzeit noch andauert. Auf Basis dieses Produktkataloges erfolgte eine Zeiterfassung hinsichtlich der Arbeitszeitanteile, die auf die einzelnen Produkte verwendet werden. Zur Wahrung datenschutzrechtlicher Belange der Beschäftigten erfolgte eine Auswertung der Daten selbstverständlich ohne Personenbezug und auf der Aggregationsebene der Arbeitsgruppen. Die Auswertung sowohl der quantitativen als auch der qualitativen Ergebnisse dieser produktbezogenen Erhebungen wurden in einem Workshop aufgearbeitet. Mittels einer Portfolio-Analyse, die auf die Entwicklungsfähigkeit der einzelnen Produkte und deren Beitrag zum Gesamterfolg der Behörde abstellte, konnten diese Ergebnisse noch verfeinert und ergänzt werden. Aus diesem Gesamtbild und Wirkungsgefüge des behördlichen Handelns kristallisierte sich ein Stärken-Schwächen-Profil heraus, das mit den Tätigkeits- und Arbeitszeitschwerpunkten der Zeiterfassung kontrastiert wurde. Dies wiederum lieferte die Grundlage zur Entwicklung einer Soll-Struktur des behördlichen Handelns, wobei in Teilbereichen ein Fort- und Weiterbildungsbedarf im Rahmen dieses Anpassungsprozesses identifiziert wurde.

[212] Dies war nur dadurch möglich, dass uns von der Senatsverwaltung für Inneres ein erfahrener Regierungsrat z. A. zur Verfügung gestellt war.

Um das Zusammenspiel zwischen einzelnen behördlichen Maßnahmen zum Datenschutz und zwischen den einzelnen Sachgebieten auch auf der Ebene der Aufbauorganisation zu verbessern, wurde eine veränderte Arbeitsorganisation gefunden und umgesetzt, bei der jeweils drei Referenten/Referentinnen in neu geschaffenen Arbeitsgruppen zusammenarbeiten, in denen sie ihre Aufgaben durch Zielvorgaben gesteuert eigenverantwortlich ausfüllen und wahrnehmen.

6.3 Zusammenarbeit mit dem Abgeordnetenhaus

Eine Änderung hat die Behandlung der Jahresberichte im Abgeordnetenhaus erfahren. Während in den Vorjahren der Jahresbericht nach Eingang der Stellungnahme des Senats im Plenum besprochen wurde und dabei der Datenschutzbeauftragte die Gelegenheit hatte, in einer Rede Stellung zu nehmen[213], wird nach einem Beschluss des Ältestenrates der Jahresbericht künftig erst nach den Erörterungen im Unterausschuss Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung im Plenum behandelt. Dies ermöglicht, die Ergebnisse in die Diskussion einzubeziehen. Über das endgültige Verfahren muss erst noch abschließend beraten werden.

Die Beratungen im Unterausschuss unter Vorsitz des Abgeordneten Rüdiger Jakesch waren erneut sehr konstruktiv. In insgesamt 12 Sitzungen wurde eine Vielzahl von Themen aus den Jahresberichten 1996 und 1997, aber auch Besprechungswünsche aus dem Parlament behandelt. Auch in anderen Ausschüssen des Hauses wurde erneut unser Rat gesucht.

6.4 Kooperation mit anderen Datenschutzbehörden

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 24 Abs. 4 BlnDSG). In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr in Wiesbaden unter dem Vorsitz des Hessischen Datenschutzbeauftragten Dr. Rainer Hamm zum 55. (19./20. März) und 56. Mal (5./6. Oktober) tagte, bündelt sich die Zusammenarbeit. Die Beschlüsse, die in der Regel auf der Arbeit mehrerer fachspezifischer, auf die einzelnen Länder aufgeteilter Arbeitskreise beruhen, sind häufig wegweisend für die Fortentwicklung des Datenschutzes. Im vergangen Jahr waren Gegenstand derartiger Beschlüsse die Geldkarte, das digitale Fernsehen, das Auskunftsverhalten des Bundesamtes für Finanzen, die Modernisierung des Datenschutzes, Datenschutzprobleme bei der Justiz, die Weitergabe von Meldedaten an Adressbuchverlage und Parteien sowie die Entwicklungen im Sicherheitsbereich[214]. 1999 übernimmt den Vorsitz der Landesbeauftragte von Mecklenburg-Vorpommern, Dr. Werner Kessel. Unter den Arbeitskreisen der Konferenz ist der unter seiner Leitung tagende Arbeitskreis Technik besonders aktiv, der wiederum mehrere Arbeitspapiere zu technisch-organisatorischen Maßnahmen des Datenschutzes vorgelegt hat[215].

Für den Bereich der Aufsicht im privaten Bereich wird die Koordinierung im Düsseldorfer Kreis, dem Gremium der Obersten Aufsichtsbehörden für den Datenschutz, wahrgenommen, der sich ebenfalls zweimal im Jahr, stets in Düsseldorf unter Vorsitz des Innenministeriums, trifft. Auch hier nehmen wir aktiv teil; in zwei Arbeitsgruppen – Teledienste und Telekommunikation[216] und Internationaler Datenverkehr[217] – führt der Berliner Datenschutzbeauftragte den Vorsitz.

Seit mit dem Berliner Bildschirmtexterprobungsgesetz von 1981 das Telekommunikationsrecht neue Wege eingeschlagen hat, ist der Berliner Datenschutzbeauftragte auf dem Gebiet des Datenschutzes bei den damals so und heute wieder so genannten Neuen Medien besonders engagiert. Ihm wurde von Anfang an von der Konferenz der Vorsitz des Arbeitskreises Medien übertragen. Im Laufe der Jahre wurde hier eine Vielzahl von Stellungnahmen erarbeitet, die zum großen Teil in der rechtlichen Ausgestaltung des heutigen Telekommunikationsrechts ihren Niederschlag gefunden haben. Aufgrund seines Engagements in den vergangenen Jahren wurde der Vorsitz in diesem Arbeitskreis von der Konferenz dem Brandenburgischen Landesbeauftragten Dr. Dix übertragen.

Beim Berliner Datenschutzbeauftragten bleibt der Vorsitz der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation, die ebenfalls seit vielen Jahren im Rahmen der Internationalen Konferenz der Datenschutzbeauftragten tagt und eine Reihe international geachteter Dokumente erarbeitet hat, zuletzt in den Sitzungen in Hong Kong am 14./15. April sowie in Berlin am 9./10. November[218].

Die Internationale Konferenz der Datenschutzbeauftragten selbst tagte im vergangenen Jahr am 16./17. September in Santiago de Compostela; der Berliner Datenschutzbeauftragte war um einen Beitrag zur Datensicherheit in Datenbanken gebeten worden.

213 vgl. JB 1997 Anlage Nr. 1; JB 1996 Anlage Nr. 1
214 vgl. Anlagenband „Dokumente zum Datenschutz 1998“, Teil B

215 zuletzt z. B. die Neufassung der „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ (9/98). Zahlreiche weitere Orientierungshilfen und Ausarbeitungen zum technischen Datenschutz finden sich in den Broschüren „Technik und Datenschutz“ (12/96) und „Datenschutzfreundliche Technologien“ (1/98) des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern.
216 vgl. 5.
217 vgl. 4.7
218 vgl. 5.1

6.5 Öffentlichkeitsarbeit

Der Berliner Datenschutzbeauftragte ist bestrebt, für seine Öffentlichkeitsarbeit das breite Spektrum der Medien zu nutzen. In Fernseh- und Radiointerviews haben wir die Gelegenheit wahrgenommen, um zeitnah Themen des Datenschutzes zu diskutieren, die für eine breite Öffentlichkeit von Interesse sind. Darüber hinaus haben wir mehrfach in *Erklärungen an die Presse* die Position des Datenschutzes öffentlich vertreten.

Wir haben u. a. Stellung bezogen,

- mit Forderungen für einen Politikwechsel zum wirksameren Schutz der Privatsphäre,
- zu Grundrechtseingriffen durch Gendatei, Schleierfahndung, Sozialamtsfalle,
- zur Benachrichtigungsflut der Polizei über Speicherungen im Informationssystem, ausgelöst durch die Vernachlässigung von Prüf- und Löschungsfristen,
- zu den rechtsstaatlichen Risiken bei der Einigung über den Lauschangriff,

und informiert über

- den unmittelbaren Anwendungsbereich der Europäischen Datenschutzrichtlinie,
- die Risiken einer Teilnahme an „Verbraucherbefragungen“ und „Kettenbrief-Aktionen“,
- die Möglichkeit, unerwünschte Wahlwerbung zur Bundestagswahl am 27. September 1998 zu verhindern.

In unserer Reihe *„Materialien zum Datenschutz“* sind zwei neue Hefte erschienen. Auf große Resonanz ist die Broschüre *„Personal Computer und Datenschutz – Materialien 25 zum Datenschutz“* gestoßen. Sie beschäftigt sich ausführlich mit den Aspekten der IT-Sicherheit und des Datenschutzes beim Einsatz isolierter oder vernetzter PCs. Der Band *„Das Internet – Ende des Datenschutzes? – Materialien 26 zum Datenschutz“* beinhaltet die Vorträge, die im Rahmen des gleichnamigen Symposiums am 1. September 1997 aus Anlass der Internationalen Funkausstellung gehalten wurden.

Aufgrund der großen Nachfrage haben wir das zeitweise vergriffene *Datenscheckheft* neu aufgelegt. Es gibt mit Musterbriefen Hilfestellung bei der Wahrnehmung von Datenschutzrechten. Es enthält z. B. Schreiben, mit denen die Zusendung von Werbematerialien eingeschränkt, sowie Schreiben, mit denen Auskunft bzw. Akteneinsicht bei der Polizei, beim Verfassungsschutz, bei Krankenkassen, Ärzten, Sozialämtern und der SCHUFA beantragt werden kann.

Neben den genannten, traditionellen Formen der Öffentlichkeitsarbeit gewinnt die Präsentation von Informationen im *Internet* zunehmend an Bedeutung. Wir haben dies frühzeitig erkannt und bieten unter „www.datenschutz-berlin.de“ seit fast drei Jahren eine ständig wachsende Sammlung von nationalen und internationalen Dokumenten, Nachrichten, Terminhinweisen usw. zum Datenschutz an. Auch die von uns herausgegebenen Broschüren und Informationsmaterialien sind als Text (und/oder als Download-Datei) in unserem Internetprogramm abrufbar. Als besonderen Service informieren wir seit Juni 1998 im *Privacy Magazine „prima“* regelmäßig – an Wochentagen täglich – über die datenschutzrelevante Berichterstattung in einer (von uns) ausgewählten Berliner und überregionalen (deutschen) Presse.

Das große Interesse, auf das unser Internetprogramm weltweit gestoßen ist, war Anlass dafür, den Inhalt (Stand: Oktober 1998) auf einer CD-ROM *„Datenschutz in Berlin – Edition 1998“* zu veröffentlichen. Damit liegt nicht nur ein umfassendes Nachschlagwerk zu datenschutzrechtlichen Fragen der letzten Jahre vor, das auch ohne Internetanschluss genutzt werden kann, abrufbar sind auch praktische Ratschläge (z. B.: Wie schreibe ich an Behörden? Wie erhalte ich Auskunft über Daten, die zu meiner Person gespeichert sind? usw.) sowie Anschriften von deutschen und ausländischen Stellen, die sich mit dem Datenschutz beschäftigen.

In der Vergangenheit haben wir großen Wert darauf gelegt, unsere Broschüren und Informationsmaterialien kostenlos (bei Versand gegen Erstattung der Portokosten) auszugeben. Aufgrund der angespannten Haushaltslage haben wir 1998 erstmals versucht, das Heft „Das Internet – Ende des Datenschutzes? Materialien 26 zum Datenschutz“ und die CD-ROM „Datenschutz in Berlin – Edition 1998“ gegen eine Schutzgebühr von jeweils 10 DM abzugeben. Ob die erzielten Einnahmen den hohen Verwaltungsaufwand rechtfertigen, ist allerdings fraglich.

Berlin, 17. März 1999

Prof. Dr. Hansjürgen Garstka,
Berliner Datenschutzbeauftragter

Anlage 1

Verzeichnis der vom Berliner Datenschutzbeauftragten herausgegebenen Informationsmaterialien (Stand: März 1999)

Der Berliner Datenschutzbeauftragte hält eine Vielzahl von Informationsmaterialien bereit, die bei Bedarf angefordert werden können. Einzelheiten – insbesondere zur aktuellen Verfügbarkeit der Materialien – sind der nachfolgenden Übersicht zu entnehmen. Der überwiegende Teil der angebotenen Broschüren ist auch als HTML- oder Download-Datei in unserem Internetprogramm **„http://www.datenschutz-berlin.de“** zum Abruf bereitgestellt. Eine Versendung der Materialien kann nur gegen Erstattung der Portokosten (1,50 DM für eine Broschüre bzw. 2,50 DM für mehrere Broschüren sind als Briefmarken der Bestellung beizufügen) erfolgen.

Jahresberichte des Berliner Datenschutzbeauftragten

Der Berliner Datenschutzbeauftragte hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister von Berlin jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Seit 1990 veröffentlicht der Berliner Datenschutzbeauftragte diesen Bericht als Bürgerbroschüre, um ihn auch der allgemeinen und interessierten Öffentlichkeit zugänglich zu machen.

	Jahresberichte des Berliner Datenschutzbeauftragten	Broschüre	Internet HTML-Textdatei	Internet Download-Datei
1990	Jahresbericht des Berliner Datenschutzbeauftragten	X		
1992	Jahresbericht des Berliner Datenschutzbeauftragten	X		
1993	Jahresbericht des Berliner Datenschutzbeauftragten	X		
1994	Jahresbericht des Berliner Datenschutzbeauftragten	X	X	
1995	Jahresbericht des Berliner Datenschutzbeauftragten	X	X	X
1996	Jahresbericht des Berliner Datenschutzbeauftragten	X	X	X
1997	Jahresbericht des Berliner Datenschutzbeauftragten	X	X	X
1998	Jahresbericht des Berliner Datenschutzbeauftragten	X	X	X

Datenscheckheft 1998

Das Datenscheckheft enthält Musterschreiben, mit denen sich die/der Betroffene an – vornehmlich Berliner – Behörden und andere Stellen wenden kann, um ihre/seine Datenschutzrechte (z. B. ihr/sein Recht auf Auskunft über die zu ihrer/seiner Person gespeicherten Daten) auf diese Weise eigenständig wahrnehmen zu können. Im Internet ist das Datenscheckheft unter „http://www.datenschutz-berlin.de/infomat/datensch/inhalt.htm“ abrufbar.

Berliner Informationsgesetzbuch

Die Forderung des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983, die Verarbeitung von personenbezogenen Daten in der öffentlichen Verwaltung normenklar zu regeln, hat dazu geführt, dass sich datenschutzrechliche Regelungen in einer Vielzahl von Gesetzen wieder finden. Das Berliner Datenschutzgesetz, das den Datenschutz bei Behörden und anderen öffentlichen Stellen regelt, setzt diese Forderung konsequent um und lässt die Erhebung, aber auch andere Formen der Datenverarbeitung nur noch zu, wenn eine derartige spezialgesetzliche Rechtsgrundlage besteht. Die wichtigsten datenschutzrechtlichen Regelungen für das Land Berlin werden vom Berliner Datenschutzbeauftragten seit 1993 in einer Textsammlung, dem Berliner Informationsgesetzbuch, herausgegeben.

	Berliner Informationsgesetzbuch	Broschüre	Internet HTML-Textdatei	Internet Download-Datei
Teil 1 - Heft 1	Berliner Datenschutzgesetz (4. Auflage 1997)	X	X	X
Teil 1 - Heft 2	Bundesdatenschutzgesetz (3. Auflage 1998)	X	in Vorb.	in Vorb.
Teil 1 - Heft 3	Besonderes Berliner Datenschutzrecht (1. Auflage 1995)		X	X
Teil 2 - Heft 1	Allgemeines Sicherheits- und Ordnungsgesetz (2. Auflage 1995)	X	X	X
Teil 2 - Heft 2	Meldegesetz (1. Auflage 1994)		X	X
Teil 3 - Heft 1	Schutz der Sozialdaten (2. Auflage 1998)	in Vorb.	in Vorb.	in Vorb.
Teil 4 - Heft 1	Datenschutz in der Schule (2. Auflage 1996)	X	X	X

Datenschutz in Berlin – Edition 1998[1)]

Das große Interesse, auf das unser Internetprogramm weltweit gestoßen ist, war Anlass dafür, den Inhalt (Stand: Oktober 1998) auf einer CD-ROM „Datenschutz in Berlin – Edition 1998“ zu veröffentlichen. Die CD-ROM enthält die Tätigkeitsberichte des Berliner Datenschutzbeauftragten, aktuelle Datenschutznachrichten, Hintergrundinformationen, die wesentlichen Rechtsvorschriften sowie nationale und internationale Dokumente zum Datenschutz. Sie ist nicht nur ein umfassendes Nachschlagewerk zu datenschutzrechtlichen Fragen der letzten Jahre, abrufbar sind auch praktische Ratschläge (z. B.: Wie schreibe ich an Behörden? Wie erhalte ich Auskunft über Daten, die zu meiner Person gespeichert sind? An welche Stelle kann ich mich wegen Verletzung meiner Datenschutzrechte wenden?) und Anschriften von deutschen und ausländischen Stellen, die sich mit dem Datenschutz befassen.

1) nur gegen eine Gebühr erhältlich.

Schriftenreihe „Materialien zum Datenschutz“

In der Schriftenreihe „Materialien zum Datenschutz“ werden ausgesuchte Teilbereiche des Datenschutzes behandelt. Die einzelnen Hefte befassen sich jeweils mit einem Schwerpunktthema (z. B. Datenschutz bei Telekommunikation und Medien oder Datenschutz in der Schule). Sie geben einen Überblick über die damit verbundenen relevanten datenschutzrechtlichen Aspekte und informieren die interessierte Öffentlichkeit über den aktuellen Diskussionsstand auf nationaler und internationaler Ebene.

	Materialien zum Datenschutz	Broschüre	Internet HTML-Textdatei	Internet Download-Datei
Nr. 1	Urteil des BVerfG zum Volkszählungsgesetz 1983 (3. Auflage 1992)	X	X	
Nr. 2	Datenschutz in Berlin, Jahresberichte 1979 - 1983	X		
Nr. 10	Datenschutz in Berlin, Jahresberichte 1984 - 1989	X		
Nr. 14	Datenschutz bei Telekommunikation und Medien (3. Auflage 1993)	X	X	X
Nr. 16	Informationen zum Berliner Dateienregister (2. Auflage 1994)	X		
Nr. 17	Datenschutz in der Schule - Ein Leitfaden für Schuldatenschutzbeauftragte (1. Auflage 1993)	X		
Nr. 18	Datenschutz in Wissenschaft und Forschung (1. Auflage 1994)		X	X
Nr. 20	Mobilfunk und Datenschutz (1. Auflage 1994)		X	X
Nr. 21	Datenschutz bei Telekommunikation und Medien 1993/1994 (1. Auflage 1995)		X	X
Nr. 22	Multimedia und Datenschutz (1. Auflage 1995)	X	X	X
Nr. 23	Medien und Persönlichkeitsschutz (1. Auflage 1996)	X	X	X
Nr. 24	Internationaler und Europäischer Datenschutz (1. Auflage 1996)	X	X	X
Nr. 25	Personal Computer und Datenschutz (1. Auflage 1997)	X	X	X
Nr. 26	Das Internet - Ende des Datenschutzes? (1. Auflage 1998)	X(1)	in Vorb.	X

(1) nur gegen eine Gebühr erhältlich.

Anlage 1

Anlage 2

Auszug aus dem Geschäftsverteilungplan des Berliner Datenschutzbeauftragten

Prof. Dr. Hansjürgen Garstka	**Berliner Datenschutzbeauftragter**
Cristina Vecchi	Sekretariat
	Zentraler Bereich
Prof. Dr. Hansjürgen Garstka	Bereichsleiter
	Zentrale Aufgaben
Birgit Saager	Arbeitsgebiete: Arbeit und Frauen, Arbeitnehmerdatenschutz
Anja-Maria Gardain	Arbeitsgebiete: Internationaler und europäischer Datenschutz, Verkehr, Justitiariat
Dipl. Informatiker Sven Mörs	Arbeitsgebiet: Telekommunikation und Medien
Dipl. Germanistin Laima Nicolaus	Sekretariat, Bibliothek, Rechtsprechung
	Allgemeine Verwaltung
Doris Werth	Büroorganisation, Haushaltsplanung und -bewirtschaftung
Alexandra Trost	Personalsachbearbeitung, Beschaffungswesen, Hausverwaltung
Monika Klößing	Sekretariat, Rechnungsstelle
	Bereich Recht
Claudia Schmid	Vertreterin des Datenschutzbeauftragten, Bereichsleiterin, Arbeitsgebiete: Datenschutzrecht, Nachrichtendienste, Verfassungsorgane, Presse- und Öffentlichkeitsarbeit, Pressesprecherin

	Recht I
Dr. Ulrich von Petersdorff	Arbeitsgebiete: Gesundheit und Soziales, Kultur
Dipl. Volkswirt Dr. Rainer Metschke	Arbeitsgebiete: Schule, Wissenschaft, Forschung und Statistik
Dagmar Hartge, Christina Heine	Arbeitsgebiet: Wirtschaft
Kerstin Göhler	Sekretariat
	Recht II
Volker Brozio	Arbeitsgebiete: Bauen und Wohnen, Stadtentwicklung und Umweltschutz, Inneres (Ausländerangelegenheiten), Redaktion von Veröffentlichungen (auch Internet)
Anja Thomsen	Arbeitsgebiete: Finanzen, Justiz
Detlef Schmidt	Arbeitsgebiete: Bürgerberatung, Inneres, Bezirksämter
Sabine Krissel	Sekretariat
	Bereich Informatik
Dipl. Informatiker Hanns-Wilhelm Heibey	Vertreter des Datenschutzbeauftragten, Bereichsleiter, Grundsatzfragen des technischen Datenschutzes, Methoden der informationstechnischen Sicherheit, Arbeitsgebiete: Recht und Politik der Informationstechnik, Spezielle Anwendungen (Komplexe IT-Verfahren, Chipkarten)
Nicole Müller	Sekretariat, Führung der Dateienregister, Informationsmaterial
	Informatik I
Dipl. Physiker Joachim Laß	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Proprietäre Systeme, Sicherheit in Rechenzentren), nicht-automatisierte Datenverarbeitung

Jürgen Horn	Arbeitsgebiet: Organisation des Datenschutzes (Führung der Dateienregister, Betreuung der betrieblichen und behördlichen Datenschutzbeauftragten, Koordination von Beratung und Prüfung), Behördlicher DSB
Dipl. Informatiker (FH) Ralf Hauser	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Personalcomputer, PC-Netze)
	Informatik II
Dipl. Informatikerin Ursula Meyer zu Natrup	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Kommunikationssysteme), Spezielle Anwendungen (Bürokommunikation), Frauenvertreterin
Carsten Schmidt	Arbeitsgebiete: Sicherheit der Informationstechnik und informationstechnische Verfahren (Offene Client-Server-Systeme)
Frank Holzkamp	Realisierung des Internetangebots
André Drescher	Systemverwaltung
Berliner Datenschutzbeauftragter	**Pallasstraße 25, 10781 Berlin, Telefon: (0 30) 78 76 88 44, Telefax: (0 30) 2 16 99 27, E-mail: mailbox@datenschutz-berlin.de, Internet: www.datenschutz-berlin.de**
Stand: März 1999	

Abkürzungsverzeichnis

ABlEG	Amtsblatt der europäischen Gemeinschaft
AG BSHG	Ausführungsgesetz Bundessozialhilfegesetz
AGGVG	Ausführungsgesetz zum Gerichtsverfassungsgesetz
Aghs.-Drs.	Abgeordnetenhaus-Drucksache
AKS	Automatisierte Kaufpreissammlung
AO	Abgabenordnung
ASOG	Allgemeines Sicherheits- und Ordnungsgesetz Berlin
AULAK	Automatisches Verfahren Land-, Amts- und Kammergericht
AuslG	Ausländergesetz
AV BSÜG	Ausführungsvorschriften zum Berliner Sicherheitsüberprüfungsgesetz
AZG	Aufgabenzuständigkeitengesetz
BABS	Bahnreise-Bestell-Service
BASIS	Berliner Automatisiertes Sozialhilfe-Interaktions-System
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BerlBetrDatVO	Verordnung über die Verarbeitung personenbezogener Daten bei den Berliner Stadtreinigungsbetrieben, den Berliner Verkehrsbetrieben und den Berliner Wasserbetrieben
BetrVG	Betriebsverfassungsgesetz
BfA	Bundesanstalt für Angestellte
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt
BlnDSG	Berliner Datenschutzgesetz
BR-Drs.	Bundesrats-Drucksache
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSÜG	Berliner Sicherheitsüberprüfungsgesetz

BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidungen
BVG	Berliner Verkehrsbetriebe
BWB	Berliner Wasserbetriebe
DB	Deutsche Bahn AG
DDR	Deutsche Demokratische Republik
DNA-Analyse	(Deutsch: DNS) Desoxyribonu[se]kleinsäure-Analyse
DNS	Domain Name Server
DV-Programm	Datenverarbeitungsprogramm
DV-Projekt	Datenverarbeitungsprojekt
DV-System	Datenverarbeitungssystem
DVD	Digital Versatile Disk
DVO-BauGB	Durchführungsverordnung zum Baugesetzbuch
DZM	Deutsches Zentralregister für kindliche Hörstörungen
ed-Maßnahme	erkennungsdienstliche Maßnahme
EG	Europäische Gemeinschaft
EU	Europäische Union
EUGH	Europäischer Gerichtshof
FAG	Fernmeldeanlagengesetz
FörderVO	Rechtsverordnung zur sozialpädagogischen Förderung
FÜV	Fernmeldeüberwachungsverordnung
GAA	Geldausgabeautomaten
GAA-Online	Gutachterausschuss-Online im Internet
GAN	Global Area Network
GBO	Grundbuchordnung
GenG	Genossenschaftsgesetz
GG	Grundgesetz für die Bundesrepublik Deutschland
GVBl.	Gesetz- und Verordnungsblatt des Landes Berlin
GVG	Gerichtsverfassungsgesetz
GwG	Geldwäschegesetz
HR	Human Resources
IBB	Investionsbank Berlin

IPV	Integrierte Personalverwaltung
ISDN	Integrated Services Digital Network
ISO	International Organization für Standardization
IT	Informationstechnik
IT-KAB	IT-Koordinations- und Beratungsausschuss
IuK-Technik	Informations- und Kommunikationstechnik
IuKDG	Informations- und Kommunikationsdienste-Gesetz
IZ-Steufa	Informationszentrale für den Steuerfahndungsdienst
JB	Jahresbericht
JGG	Jugendgerichtsgesetz
JUKOS	Justiz-Kostenbearbeitung
Kfz	Kraftfahrzeug
KG	Kammergericht
KOKA	Geschäftsstellenautomation in Konkurssachen
KOM	Dokument der Europäischen Kommission
LBB	Landesbank Berlin
LBG	Bundesbeamtengesetz
LEA	Landeseinwohneramt
LHO	Landeshaushaltsordnung
LIT	Landesbetrieb für Informationstechnik
LStatG	Landesstatistikgesetz
MAN	Metropolitan Area Network
MDStV	Mediendienste-Staatsvertrag
MeldeG	Meldegesetz
MRRG	Melderechtsrahmengesetz
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NJWE-MietR	Neue Juristische Wochenschrift, Entscheidung im Mietrecht
NSA	National Security Agency
OECD	Organization of Economic Cooperation and Development
OLG	Oberlandesgericht
OSAV	Online-Schwerbehinderten-Anwendungs-Verfahren

OSI	Open Systems Interconnection
PStG	Personenstandsgesetz
PStV	Personenstandsverordnung
PsychThG	Psychotherapeutengesetz
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SGB	Sozialgesetzbuch
SIS	Stadtinformationssystem
SOZhiDAV	Sozialhilfedatenabgleichsverordnung
SQL	Standard QUERY Language
Stasi	Staatssicherheitsdienst
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUÄndG	Stasi-Unterlagen-Änderungsgesetz
StVÄG	Strafverfahrensänderungsgesetz
StVG	Strafverfahrensgesetz
StVollzÄndG	Strafvollzugsänderungsgesetz
SWI	Süd-Westdeutsche Inkasso-KG
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TKUV	Telekommunikations-Überwachungsverordnung
VermG	Gesetz über das Vermessungswesen in Berlin
VerwrefG	Verwaltungsreformgesetz
VG Bln	Verwaltungsgericht Berlin
VS-NfD	Verschlusssache – Nur für den Dienstgebrauch
VwVfG	Verwaltungsverfahrensgesetz
WASt	Deutsche Dienststelle für die Benachrichtigung der nächsten Angehörigen von Gefallenen der ehemaligen deutschen Wehrmacht
WoBauG	Wohnungsbaugesetz
WoBindG	Wohnungsbindungsgesetz
WWW	World Wide Web
ZERV	Zentrale Ermittlungsstelle für Regierungs- und Vereinigungskriminalität
ZKA	Zentraler Kreditausschuss
ZPO	Zivilprozessordnung

Stichwortverzeichnis

Stichwortverzeichnis